HENRY FLOOD

ADEQUATE PROTECTION:
AN EXAMINATION OF TRANSBORDER DATA PROTECTION STANDARDS IN THE EUROPEAN UNION

LLM THESIS

FACULTY OF LAW
UNIVERSITY OF OTAGO
2017
Table of contents

Table of Contents ................................................................. 1
Abstract .................................................................................. 5
Word Length ........................................................................... 5
Acknowledgments ...................................................................... 5

I INTRODUCTION ..................................................................... 6

II LITERATURE REVIEW .......................................................... 9
    A How is Privacy Conceptualised in Europe and the United States? .... 9
        1 Privacy in Europe ............................................................. 10
        2 Privacy in the United States .............................................. 12
        1 Privacy ................................................................. 14
        2 Politics .................................................................... 16
        3 Economics ................................................................ 20
    C What is Personal Data? ..................................................... 24
        1 The United States Approach ........................................... 24
        2 Directive and the Regulation ......................................... 26
    D Facebook ......................................................................... 29
    E Key Points ....................................................................... 33

III INTRODUCTION TO ADEQUACY ......................................... 35
    A What are the Adequacy Principles in the Directive? ................. 39
        1 Purpose Limitation .................................................... 40
        2 Data Quality and Proportionality .................................. 42
        3 Transparency .......................................................... 43
        4 Security ..................................................................... 44
        5 Rights of Access, Rectification and Opposition ................. 44
        6 Restrictions on Onward Transfers .................................. 45
        7 Sensitive Data ........................................................... 45
        8 Direct Marketing ....................................................... 46
        9 Automated Individual Decision Making ......................... 46
10 Procedural and Enforcement Mechanisms...........................................47
B Discretion in Assessing Compatibility with Principles..........................47
C Key Points..........................................................................................49

IV How Was Adequacy Shaped by the Safe Harbour Agreement?...........50
A What Was the Safe Harbour?.................................................................50
B Substantive Protections........................................................................52
   1 Data Quality.....................................................................................53
   2 Legitimate Processing.......................................................................54
   3 Onward Transfer...............................................................................54
   4 Rights of Data Subjects.....................................................................55
   5 Independence....................................................................................56
C Preliminary Conclusions on the Safe Harbour.....................................57

V INTRODUCTION TO SCHREMS.............................................................58
A Who Is Max Schrems and What Action Did He Take against Facebook?...58
B Interlocutory Judgment of the Irish High Court....................................61
   1 General Remarks..............................................................................61
   2 Issue of Frivolity..............................................................................63
   3 What Was Referred to the Court of Justice?......................................63

VI SCHREMS IN THE EUROPEAN COURT OF JUSTICE..........................65
A Framework for Analysis: Four European Essential Guarantees............67
B The Powers of the National Supervisory Authorities............................68
C Safe Harbour Validity: Detection and Supervisory Mechanisms.............72
   1 Applicable law.................................................................................72
   2 Federal Trade Commission..............................................................74
   3 Alternative Dispute Resolution Mechanisms....................................75
   4 Conclusions.....................................................................................76
C Safe Harbour Validity in Light of the Derogations and Limitations: Clear,
   Precise and Accessible.......................................................................78
D Safe Harbour Validity in Light of Derogations and Limitations: Necessity
   and Proportionality..........................................................................81
   1 Test One: Pressing Social Needs.....................................................83
(a) Whether the Measure Mitigates against Harm ........................................ 84
(b) What Are the Broader Societal, Historical and Political Views? ........ 86
(c) Whether Opposition Views Have Been Sufficiently Taken Into Account .... 87
(d) Conclusion on the Pressing Social Need Test ....................................... 88
2 Test Two: Proportionality ........................................................................ 88
(a) Limited in Scope .................................................................................. 89
(b) Safeguards .......................................................................................... 91
(c) Severity of the Issue and Harm Which Society Could Be Exposed to ...... 91
(d) Benefits over Proposed Measures ......................................................... 93
(e) Conclusion on Proportionality test ....................................................... 94
3 Conclusion on Safe Harbour Validity in Light of Necessity

and Proportionality ................................................................................... 94
E Key Points .............................................................................................. 95

VII FUNDAMENTAL RIGHTS JURISPRUDENCE ........................................ 97
A Further Case Study: Positive Adequacy Decision for Passenger Name Record

Data ............................................................................................................. 101
B Fundamental Rights in the European Union Generally ......................... 104

1 Economic Issues ..................................................................................... 105
2 Primacy Issues ....................................................................................... 107
C Key Points .............................................................................................. 113

VIII EUROPEAN UNION’S DATA PROTECTION DIRECTION .............. 115
A The General Data Protection Regulation .............................................. 115

1 Right to Data Portability .......................................................................... 118
2 Right to an Explanation .......................................................................... 120
3 Privacy by Design and Default ............................................................... 122
B The Privacy Shield .................................................................................. 124

IX WHERE TO FROM HERE? ................................................................. 128
A Harms of Data Insecurity ......................................................................... 132
B Why Can Adequacy and the Regulation Assist? ....................................... 136
C What Specific Improvements Could Be Made? ....................................... 137
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Organisational</td>
<td>138</td>
</tr>
<tr>
<td>2 Technical</td>
<td>141</td>
</tr>
<tr>
<td>X CONCLUSION</td>
<td>146</td>
</tr>
<tr>
<td>XI CASES, LEGISLATION AND BIBLIOGRAPHY</td>
<td>150</td>
</tr>
<tr>
<td>A Table of Cases</td>
<td>150</td>
</tr>
<tr>
<td>B Table of Legislation and International Instruments</td>
<td>152</td>
</tr>
<tr>
<td>C Books</td>
<td>154</td>
</tr>
<tr>
<td>D Essays and Chapters in Books</td>
<td>156</td>
</tr>
<tr>
<td>E Journal Articles</td>
<td>156</td>
</tr>
<tr>
<td>F European Union Materials</td>
<td>161</td>
</tr>
<tr>
<td>G Internet Resources</td>
<td>163</td>
</tr>
<tr>
<td>H Papers and Reports</td>
<td>167</td>
</tr>
<tr>
<td>I Other</td>
<td>169</td>
</tr>
</tbody>
</table>
Abstract

This paper considers the requirements of “adequate protection” of transborder data flows in the European Union.

Word Length

The text of this paper (excluding abstract, table of contents, footnotes and bibliography) comprises approximately 41,000 words.

Acknowledgements

Particular thanks to Professor Paul Roth for his sagacious guidance and insightful suggestions; to my family for their sense of humour and judicious proofreading; to Edward Snowden for his sacrifice; and to Max Schrems for his endurance.
I INTRODUCTION

Data processing is driving an information explosion, redefining how we interact in a progressively connected world.

However the rapid, volatile evolution of the online environment is causing tensions in the law. Issues have escalated with the emergence of Big Data, cloud computing, social networking and mass surveillance.

The ability to process data internationally has taken on profound cultural and social significance. We increasingly use data to speak, socialise, organise and do business—how should the law respond?

The Council of Europe, Organisation for Economic Cooperation and Development and United Nations were first to develop legal instruments for regulating data processing however it was the European Union (EU) which was initially the most successful,¹ with the Data Protection Directive (95/46/EC) (the Directive).²

These instruments were developed when international data flows were exceptional and mostly concerned technical rather than personal data.³ However the structure of the internet is no longer point to point transmissions within a country but international transfers of personal data through reticular networks.

This thesis will examine the Directive’s attempt to regulate these international transfers in the EU context. The examination is an intricate exercise in legal pluralism. A multiplicity of distinct normative systems interact—public law, human rights law, economic regulation, privacy law, international law, regional agreements and national security law all compete for primacy in a shifting legal landscape.⁴

⁴ Bygrave, above n 1, at 22.
Areas of current debate include: how to determine the applicable law when data flows between countries; how national security interests should be balanced with privacy; whether “data havens” can be used to circumvent the law; how economic goals should be balanced with privacy; whether market based solutions protect privacy better than legal regulation; and how technology can be used to protect privacy by design and default.

These concerns are without obvious answers and caused considerable debate as the Directive was negotiated. As a consequence of the legal and political compromises made the Directive is regrettably but necessarily nebulous. The core tension is revealed in its dual purposes- to protect the right to privacy and to promote the internal market of the EU through the free flow of data. These purposes can tug in opposite directions.

The EU regulation of transborder flows- personal data being processed outside the European Economic Area- is of central importance as there is concern these flows could circumvent the Directive’s protections.

“Adequacy” is the legal tool used to mitigate these concerns and protect the personal data flows. Under the Directive, Member States can transfer personal data to countries outside the European Economic Area only if the recipient country ensures an adequate level of protection of personal data (emphasis added). Unearthing and giving clarity to this complex legal standard provides the centre of mass of this thesis.

The United States was held to provide adequate protection through a scheme called the Safe Harbour. However in the recent Schrems v Data Protection Commissioner the European Court of Justice (ECJ) found the Safe Harbour invalid, drawing on Edward Snowden’s revelations of mass surveillance by the United States National Security Agency (NSA).

---

5 Bygrave, above n 1, at 56.
6 Article 1.
7 Case C-362/14 Schrems v Data Protection Commissioner (CJEU 6 October 2015) [Schrems].
This has pushed adequacy into a bubbling discourse about the right to privacy in a technological world and the limits of legislating in the interests of national security. It is to this discourse I seek to contribute.

Adequacy provides a locus for discussion as it hosts a considerable clutter of legal, political and economic disagreements. The analysis required occasions a broad perspective with economic and political components kept firmly in mind. The surface structure of adequacy is expressed in the law however a deeper understanding of its weaknesses and future requires a sharp analysis of economic and political forces.

First I will examine adequacy’s statutory meaning. Then I will examine how its meaning was shaped by the Safe Harbour and Schrems. Finally I will examine how the meaning is shaped by the new General Data Protection Regulation\(^8\) (Regulation) before looking at what the future of adequacy might entail. My research question is therefore as follows- what is the meaning of adequate protection?

---

\(^8\) Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 [Regulation].
II LITERATURE REVIEW

To contextualise and untangle the uncertainties surrounding adequacy this literature review will canvass the broad legal, economic and political landscape of the legal standard.

A How is Privacy Conceptualised in Europe and the United States?

The portability of data have precipitated a privacy culture collision between the United States and Europe.\(^9\) In order to understand why the data protection approaches are clashing in the context of transborder data flows this section will examine the privacy cultures in the two regions.

Notoriously slippery, the concept of privacy resists definition and as Professor Judith Thomson notes, “nobody seems to have any clear idea of what it is.”\(^10\) Adding to the uncertainty are the distinctive cultural particularities of what should be kept private and what deserves protection. To highlight this with jarring vulgarity anthropologists point to societies where public defecation does not offend local privacy norms.\(^11\) This shows the difficulty of using intuitionist arguments when defending privacy. Everyone has their own anxieties about privacy invasions however to a large extent they are a product of the social and legal values of the societies we participate in.\(^12\)

Privacy has been employed to protect a multitude of interests, from the rights of women, homosexuals, the use of contraceptives and the right to view pornography. However no coherent definition has materialised and some commentators argue it never will.\(^13\)

---


\(^12\) James Whitman “Two Western Cultures of Privacy: Dignity versus Liberty” (2004) 113 Yale Law Journal 1151 at 1160.

One author has caricatured the tension between the European and American approaches as coming from two foundational world views captured by Goethe and Jefferson. For Goethe, representing the European position, the development of “personality” was the “greatest blessing.” For Jefferson, representing the United States, the foundation of a free society lay in press liberty. Of course there are still threads of the European dignity approach in the United States— a relative comparison of the two cultures is required rather than a false dichotomy of dignity or liberty.

Nevertheless significant divergence exists in both the theory and practice of privacy law in the two regions. To many Europeans the American law of credit reporting seems most offensive— surely the full credit history of someone who has never defaulted should be protected from invasive rummaging. Alternatively public nudity, offensive to many Americans who treat genitals as “privates” in the full sense, is acceptable in Europe as the exposed controls the decision to reveal. These different beliefs about privacy are clashing in the ideological battle of international data transfer but they have clashed before, such as in the context of discovery.

1 Privacy in Europe

The European attitude to privacy is that it protects a “right of personality.” European privacy treats the right to respect and personal dignity as the values of supreme importance. Control over the information disclosed about oneself, called informational self-determination, is at the core of the right. It is a human right to control one’s image, name and reputation. The media is seen as a prime enemy...
with the ability to disperse information causing embarrassment, threatening dignity on the public stage.

Commentators such as Robert Kagan have popularised European dignity conceptions of privacy as a response to fascist oppression leading up to, and during, World War II. Certainly international human rights law, such as the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR), were largely a response to World War horrors and international human rights law is crucially linked with data protection law in Europe.

However Professor James Whitman provides a longer term view of privacy protecting dignity. He argues it developed from a slow agitation against exclusive hierarchical dignity on the continent. In the eighteenth and seventeenth centuries the right to respect was available in court only to high status individuals in Europe, particularly through the laws of duelling where high status individuals could defend their honour in a duel. Additionally the punishments for low status offenders, from a comparative point of view, lacked dignity. A low status offender would be hung rather than beheaded, or detained in a penal colony rather than in an apartment. The social norm that everyone should be entitled to dignity, regardless of social standing, slowly pushed the status protections reserved for the ruling classes to provide “privacy” for all. This social transformation brought dignity and status protections not only to the poorer classes and minorities, but even to prison inmates.

Early data protection legislation occurred at the national level rather than the supranational level in Europe, with Germany, Sweden, Austria, Denmark, France and

---

22 European Convention for the Protection of Human Rights and Fundamental Freedoms ETS 5 (signed 4 November 1950, entered into force 3 September 1953) [ECHR].
23 International Covenant on Civil and Political Rights 999 UNTS 171 (signed 16 December 1966, entered into force 23 March 1976) [ICCPR].
24 See Directive, art 1(1), which seeks to strengthen normative links between data protection and fundamental rights, see also Schrems.
25 Whitman, above n 12, at 1167.
26 At 1166.
Norway being the first countries, in order, to enact data protection statutes. They focused on implementing Fair Information Practices which defined core obligations for personal data processing. However it is the international agreements achieved, rather than complementary national legislation, which has given European data protection law its international prominence.

2 Privacy in the United States

Privacy law in the United States germinated from hostility towards media and a deep suspicion of the state and public officials. Rather than protecting dignity, privacy in the United States concerns liberty and freedom from state intervention, particularly in the sanctity of the home. Whitman sees American anxieties about privacy to be primarily concerned with protecting a private sovereignty within the family household. These anxieties are not exclusive to the United States however, with the Charter of Fundamental Rights of the European Union (the Charter) and the ICCPR also protecting the home from unlawful interference.

The United States Constitution does not have a specific privacy provision however the Supreme Court has found a right to privacy exists within the Bill of Rights. A host of heated political issues have been dealt with as privacy matters. For example abortion was conceived as a privacy issue in Roe vs Wade, as was homosexuality in Lawrence v Texas. Whilst some argue the flexibility of privacy to encompass such issues is a strength, others such as Professor Raymond Wacks express disquiet that it is an overstretched and weakening of privacy law. Certainly the Constitution cuts in both directions. For example the First Amendment can support privacy

---

28 Whitman, above n 12, at 1160.
30 ICCPR art 17, see also Entick v Carrington [1765] EWHC KB J98 for a common law defence of the home.
32 Lawrence v Texas, 539 US 558.
33 Wacks, above n 13, at 4.
through protection of freedom of association however it can also hinder privacy
through asserting the right to freedom of speech.\textsuperscript{34}

Crucially privacy in the United States, whilst weak when in conflict with the freedom
of the press, has enjoyed strength in the context of police or state violations. Once
violations involve state actors there seems to be greater judicial willingness to find
in favour of the plaintiffs- Whitman argues if an issue can be analogised with a state
invasion into the home, a privacy violation is particularly likely to be found.\textsuperscript{35} There
is a possibility the home invasion metaphor could be mobilised to cover mass
surveillance of transborder data flows, perhaps catalysing American enthusiasm for
stronger data protection.

However Professor Stephen Schnably argues the ideal of privacy as resisting state
power is a chimera. Rather than seeing the state as the opposition and looking to
strengthen privacy protections against the state, he argues a better focus would be
how privacy could be protected by the power of the state.\textsuperscript{36} This could provide a
well-resourced counter to the growing privacy invading ability of private economic actors. However Snowden’s revelations reduced the credibility of leading western
states- they were shown to engage in obscurantism and obfuscation regarding the
extent of their surveillance. The lack of credibility the United States has when
discussing data protection would appear to be a significant hurdle to achieving
Schnably’s ideal.

The United States also has an individual responsibility narrative. Users are expected
to protect their own privacy interests in a relatively deregulated environment. This
belief resonates with the self-help culture in which Americans are supposed to look
out for themselves. For example Professor Fred Cate believes the most effective way
of protecting privacy is through individual responsibility rather than regulation.\textsuperscript{37}
However this position suffers from the heterogeneous nature of internet users-
there is a considerable diversity in the sophistication and privacy awareness of

\textsuperscript{34} Schwartz, above n 27, at 1976.
\textsuperscript{35} Whitman, above n 12, at 1215
\textsuperscript{36} Stephen Schnably “Beyond Griswold: Foucauldian and Republican Approaches to Privacy” (1989) 102 Harv Law Rev 737 at 739.
\textsuperscript{37} Fred Cate Privacy in the Information Age (Brookings Institute, Washington, 1997) at 131.
users. It is difficult to expect all the unsophisticated young internet users in the United States to protect their privacy online, particularly when to participate in popular culture they may feel coerced into using a wide range of online services all with different privacy protections.

B What Purposes do Data Protection Law and Transborder Flows Serve?

Data protection law generally and transborder data flows specifically serve a multitude of purposes - which often conflict. For simplicity the purposes have been organised under three areas: privacy; politics; and economics. This is necessarily reductionist with some topics, such as fundamental rights, clearly including elements from more than one area.

1 Privacy

From a humanistic perspective data protection law and transborder data flow protections typically seek to protect the right to privacy. For example the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the Convention) aims to secure for individuals “respect for his rights and fundamental freedoms, and in particular his right to privacy”38 and the Directive protects “the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.”39 In the specific case of transborder flows there is a heightened risk to privacy if the recipient country has lower data protection standards than the transferring country - a so called data haven.

However privacy is not always the explicit value protected. For example data protection legislation in Europe often does not protect “privacy” but other values

---

such as “personality”\textsuperscript{40} or “personality right”\textsuperscript{41} or “personal integrity.”\textsuperscript{42} The array of values referred to hint at an underlying incoherence. Even when privacy is used explicitly, as in the Convention and Directive, the high generality of “rights and fundamental freedoms” suggests a host of values upon which justification for data protection law may be constructed.

At a broad level, Professor Alan Westin has classically outlined four functions of privacy. First, it fosters personal autonomy by allowing individuals to avoid manipulation by others. Second, it allows the removal of the social masks worn by individuals both online and offline. A young law student may be: a caring boyfriend; a motivating hockey captain; a loving grandson; a campfire entertainer; an online environmentalist; and a responsible older brother. Privacy gives rest from the emotional effort of always wearing one of those masks. Thirdly, privacy gives the opportunity to test new ideas, insulated from the criticism of others. This allows self-development and self-evaluation. Finally, privacy allows intimacy and the sharing of protected communications.\textsuperscript{43}

It is important here to note a distinction between privacy and the narrower “information privacy” that data protection law looks to protect in transborder data flows. Westin outlines that information privacy concerns a claim of an individual to determine for themselves how, when and to what extent information about them is communicated to others.\textsuperscript{44} More succinctly Professor Arthur Miller describes it as “the individual’s ability to control the circulation of information relating to him.”\textsuperscript{45} If transborder data flows are not protected then an individual’s ability to control the information circulating about him is reduced. The chilling effects of a loss of information privacy were articulated in a 1983 decision by the West German Constitutional Court. They outlined if someone cannot predict what personal information is known to others in his social situation, or what knowledge may be passed on to other parties not present, he is inhibited in his freedom to plan and

\textsuperscript{40}Federal Act on Data Protection 1992 (Switzerland), art 1(1).
\textsuperscript{41}Federal Data Protection Act 2003 (Germany), art 1(1).
\textsuperscript{42}Personal Data Act 1998 (Sweden), s 1.
\textsuperscript{43}Alan Westin Privacy and Freedom (Bodley Head Ltd, New York, 1967) at 34-35.
\textsuperscript{44}At 7.
\textsuperscript{45}Arthur Miller Assault on Privacy: Computers, Data Banks and Dossiers (University of Michigan Press, Michigan, 1971) at 40.
decide freely how to act. For example if an individual does not know whether participation in an online referendum or political movement will be registered, and he does not know whether personal risks might flow from others having knowledge of such participation, that individual’s autonomy is constrained.

Significant threats to privacy exist with modern data processing—particularly through profiling. Sir Tim Berners-Lee, creator of the World Wide Web, uses a health insurance example to highlight concerns. If a health insurance company can purchase the search queries of a user, who might have searched for books on cancer for example, the company could increase premiums. The premiums might rise even if the searcher was simply browsing for curiosity or to gather information for a friend.

Crucially the inferences drawn from algorithms are largely based on existing stereotypes, which can be further perpetuated by the processing. Individuals might not share the information they do online if they knew how it shaped their profile and therefore chance of securing credit, a job or parole. Some forms of data profiling can be particularly manipulative and invasive of privacy—such as the deliberate targeting of individuals with addiction issues.

2 Politics

Data protection law and transborder data flows interact with complex political and legal values including: human rights; national security; sovereignty; and political protest.

Human or “fundamental” rights are an increasingly important realm of data protection law. The ECHR, ICCPR and United Nations Declaration of Human Rights

---

48 At 547.
49 Alessandro Acquisti “The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines” (paper presented to OECD Conference Centre, Paris, 1 December 2010) at 74.
all protect privacy as a human right. Importantly it was the Charter which heavily influenced the case of Schrems. The court crucially found the requirements of adequacy must be considered in light of the fundamental rights guaranteed under the Charter and in particular the large number of people who would be vulnerable to having their rights infringed if their personal data was transferred to a country not ensuring adequate protection.\(^{51}\)

The court found an adequate level of protection requires a protection of fundamental rights and freedoms that is “essentially equivalent,” rather than identical, to the protection guaranteed by the Directive.\(^{52}\) The fundamental rights under the Directive were given a “high level” of protection.\(^{53}\) However as James Michael argues, human rights can be a difficult legal landscape. Critically human rights can threaten privacy in some contexts- for example freedom of expression, the right to impart information, is a human right which can act against privacy.\(^{54}\) Additionally human rights apply best in an all or nothing fashion, when they collide it can be difficult to weigh the competing interests.

National security also has a difficult relationship with adequacy. National security provides an exemption from the requirements of the Directive\(^{55}\) as well as an exemption in the Safe Harbour scheme.\(^{56}\) However as ruled in Schrems national security as an exemption can restrict protections of personal data only so far as is strictly necessary\(^{57}\) and to meet overriding legitimate interests.\(^{58}\) There has long been a tension between safeguards and the power of sovereign states to act in the interests of national security. With the incredible processing power of mass surveillance networks, the conversation over limits to acting in national security is gaining momentum in the public discourse. However there is a difficult tension between the judiciary, the legislature and the executive when the exemptions are at issue. To find a government as acting outside the national security exemption is to

---

51 Schrems, at [78].
52 At [73].
53 At [39].
55 Art 13(1)(a)
57 Schrems, at [92].
58 At [84].
attack a central core of their sovereignty- these tensions are particularly pronounced when they occur between a national government and a supranational body such as the EU.

In general online activity can create trying sovereignty and jurisdictional issues. Professor Lawrence Lessig classically refers to a situation where a group of people from multiple countries transfer data to another country’s servers to build a virtual community in cyberspace. It is an exceptionally difficult political and legal problem to decide which jurisdiction should govern- where the servers are, where the people are located, or somewhere else.59

If states can bolster their digital sovereignty and extend their online jurisdiction then their political power is increased. The United States for example, has looked to extend their online jurisdiction extra-territorially into Russia.60 The EU is certainly looking to extend their data protection norms beyond Member States. Adequacy can be viewed as a tool in this complex battle for achieving digital sovereignty- the requirements act extraterritorially by imposing obligations on data controllers and processors outside of the European Economic Area.61 Ultimately there is economic leverage for the spreading of the EU’s standard of adequacy as trading states want to access the huge European market.

From a civic point of view data protection laws can facilitate global communication, the reporting of news, safe dissemination of political viewpoints and coordinated mobilising of political protest as occurred during the Arab Spring uprising.62 If transborder data flows are not secure, or simply perceived to be unsecured, there can be a considerable chilling of the exercise of political rights and civil disobedience. Adequacy can therefore serve an important signalling function to citizens wanting to know what online activities and jurisdictions are safe. However given Snowden’s revelations of mass surveillance, it is difficult for citizens to predict

60 See US v Ivanoc 175 F Supp 2d 36 (D Conn 2001) where the United States held individual accountable under United States law for intending and causing harm in America whilst acting online from Russia.
the extent and nature of threats to personal data processed as part of the exercise of political rights.

Data protection law in the context of transborder data flows serve a crucial harmonising purpose. The Directive looks to bring about an approximation of the national laws of its Member States resulting in equivalent levels of data protection.\textsuperscript{63} If laws are harmonised then the regulatory burden of operating across jurisdictions is significantly reduced. If a company has to carefully redesign the digital services they provide in order to comply with different national regulations they may avoid countries entirely, at the very least they will incur higher costs of doing business. The harmonising of data protection law to ease transborder flows serves a clear financial purpose as well as nurturing political relationships between states.

The United States has advocated for an open internet but secretly sought to undermine encryption and conduct mass surveillance of users.\textsuperscript{64} Most countries do not have the political or economic power to oppose this American dominance—particularly as many free ride on American intelligence and military capabilities. Whilst the EU does not have jurisdiction over American agencies such as the NSA, crucially they can influence the European operations of American firms.\textsuperscript{65} From a hegemony perspective, adequacy can therefore be viewed as an ideological battleground for control of the international norms of transborder data flows. Data is an incredibly valuable asset so influence over the international norms of transborder data flow provides significant political power. Dr Michelle Frasher describes the process as “information statecraft” where there is an attempt to influence the behaviour and policies of states by acquiring or controlling data flows.\textsuperscript{66} Whilst some argue the Safe Harbour is closer to European rather than American data protection norms,\textsuperscript{67} the United States very effectively negotiated

\textsuperscript{63} Directive, recitals 8 and 9.

\textsuperscript{64} Henry Farrell and Abraham Newman “Transatlantic Data War: Europe Fights back against the NSA” (2016) 95 Foreign Aff 124 at 125.

\textsuperscript{65} Ibid.

\textsuperscript{66} Michelle Frasher and Travis Selmier II “The cross-Atlantic Tussle over Financial Data and Privacy Rights” (2013) 56 Business Horizons 767 at 768.

\textsuperscript{67} Schwartz, above n 27, at 1981.
considerable limitations, including national security exceptions and the exclusion of financial data from the scheme.\textsuperscript{68}

3 \textit{Economics}

An economic lens provides essential insight to both the background context of adequacy as well as the case of \textit{Schrems}. Both the Directive and the Regulation have economic progress as a driving purpose.\textsuperscript{69} Economics is a central concern for data protection legislation generally but holds particular importance for transborder flows - international commerce demands these flows take place.

Many technology innovations rely on transborder data flows to function, including: the internet of things; the app economy; cloud computing; Big Data; online streaming services; E-commerce; and crowdfunding.\textsuperscript{70} These technologies hold tremendous potential across multiple fields, with Big Data analytics in Google Flu Trends (predicting influenza outbreaks from aggregated search queries on Google) being an often cited success.\textsuperscript{71} Data protection law has the uncomfortable task of protecting privacy whilst still promoting these beneficial emerging technologies. There is concern too many privacy protections may hinder the development and use of these technologies. However strong privacy protections may also provide the nurturing environment Westin outlines above - cultivating imagination and inventive propensities.\textsuperscript{72} Finding a balance is crucial given the substantial gains to welfare these technologies promise. However I am concerned support for privacy in this context will be unwisely labelled technophobic and anti-progress.

Of particular consequence is the industry opposition to omnibus regulation of privacy in the United States. The same year the Directive was made industry representatives in the United States argued omnibus privacy regulation would:

\begin{itemize}
\item \textsuperscript{68} Frasher, above n 9, at 791.
\item \textsuperscript{69} Directive recital 1, Regulation recital 1.
\item \textsuperscript{71} Omer Tene and Jules Polenetsky "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) 11 Northwestern Journal of Technology and Intellectual Property 239 at 240.
\item \textsuperscript{72} Michael, above n 54, at 47.
\end{itemize}
hinder innovation; drive marketing activity off the internet; add unnecessary costs to online advertising; and distort the market definition of consumer privacy preferences.\textsuperscript{73} They argued for stripped down sectoral legislation. Benefits were expected to flow from having relatively unfettered access to consumer information—such as more relevant advertising, better fraud protection and more convenient customer services. Consent requirements were thought to burden consumers and create additional costs—perhaps a self-fulfilling prophecy in light of the unhelpful, obscure privacy policies issued by many corporations.

Industry believed market forces could and would satisfy customer privacy preferences.\textsuperscript{74} There was also a belief that excessive privacy regulation might not only raise the cost of business, but ultimately push corporations to do business outside of the United States.\textsuperscript{75} This argument may marinate American concerns about “foreigners” taking domestic jobs, or “American” jobs being lost to other countries but it is unclear whether firms gain an advantage by having lower privacy protections. Indeed under certain conditions privacy protections appear to be revenue enhancing.\textsuperscript{76} The adequacy requirements of the Directive might therefore be seen as an attraction rather than a deterrence for many business and consumers—who might not want to risk their personal data being compromised.

Nevertheless the anti-regulation position is backed by neoclassical economic scholarship. Professor Paul Rubin and Dr Thomas Lenard suggest consumer preferences for data protection can be satisfied by market forces and self-regulation rather than a legal standard like adequacy. They argue public fallout from firms misusing personal information has previously catalysed the improvement of data protection practices—presumably they believe the changes to be sufficient, widespread and enduring. However customers are often unaware of where, when

\textsuperscript{73} Ira Rubinstein “Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes” (Public Law and Legal Theory Working Paper, New York University, March 2010) at 361.
\textsuperscript{74} At 362.
\textsuperscript{75} Frasher, above n 9, at 789.
\textsuperscript{76} Janice Tsai and others “The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study” (2010) 22(2) Information Systems Research 254 at 264.
and how a data breach occurs compromising their ability to discipline the data controller by reducing their demand for services.\textsuperscript{77}

The Department of Commerce in the United States notes that an erosion of trust will retard the adoption of new technologies.\textsuperscript{78} It is difficult to know the extent to which internet users will trade off privacy and accept unscrupulous data processing in order to secure the benefits flowing from future technologies. However it appears the market for privacy tends to underprovide protection for individuals under many real world conditions such as consumers acting myopically or data subjects having incomplete information.\textsuperscript{79}

Neo-classicist Justice Richard Posner views the protection of privacy as creating inefficiencies by hiding information- under the neoclassical framework perfect information is required to achieve the correct market equilibrium.\textsuperscript{80} However the neoclassical economic scholarship is strongly contested with Professor Jerry Kang and Professor Paul Schwartz pointing to two market failures. First, information asymmetries exist as consumers are unaware how personal data are being handled and transferred online- there is also an ancillary issue of uninformed consent whereby users agree to privacy policies without knowledge of them.\textsuperscript{81} Second, there is a collective action problem as consumers are fragmented, facing concentrated costs but diffuse benefits of individually bargaining for better privacy policies.

Considering “more relevant advertising” as a benefit and consumer consent as an intrusive cost appears biased towards data controllers rather than data subjects. Some commentators even style targeted advertising as an “immensely powerful instrument for the elimination of ignorance.”\textsuperscript{82} To conceive of life’s accumulation of knowledge as the receiving of advertising appears to be an appalling degradation of

\textsuperscript{77}Rubinstein, above n 73, at 362.
\textsuperscript{78}Department of Commerce Internet Policy Task Force “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework” (Internet Policy Task Force Privacy Green Paper, 16 December 2010).
\textsuperscript{82}Howard Beales III “Consumer Protection and Behavioural Economics: To be or not to be?” (2008) 4 Competition Policy International 149 at 152.
epistemology. Nevertheless more relevant advertising as a benefit receives considerable ventilation. The advertising is seen as solving, rather than exploiting, an information asymmetry, whereby consumers overcome their lack of knowledge about new products, which is held to empower them. 83 This justification requires the highly contested foundation that humans are at the core, materialistic consumers.

Professor Curtis Taylor challenges more relevant advertising as a benefit, arguing that naïve consumers do not anticipate secondary uses of their data and can be exploited rather than empowered. 84 Given the complexity of privacy terms and conditions it is incredibly difficult for a common consumer to decipher a single privacy statement let alone rank them. From an empirical point of view the number of consumers who actually read privacy terms and conditions also undermines a market based solution - on one analysis if every American internet user read all the privacy policies of websites they use the opportunity cost of that time would be approximately USD 781,000,000,000. 85 Kang describes individuals as “largely clueless about how personal information is processed through cyberspace.” 86 Even when consumers are informed of privacy implications, there is evidence they act myopically when analysing the short term benefits of free online services and the long term costs of information revelations. 87

In summary data protection law and transborder flows seek to balance complex of diverse purposes. Privacy, innovation, sovereignty, hegemony and economic growth can all be constrained or nurtured by transborder data flows. Crucially it is adequacy that has the uncomfortable task of navigating these conflicting, dissimilar goals.

86 Kang, above n 81, at 1253.
87 Acquisti, above n 49, at 9.
C What is Personal Data?

Personal data is the fundamental unit of information privacy. The terms change across jurisdictions but “personal data” and “personally identifiable information” are foundational concepts in data protection law as they act as jurisdictional triggers. If data being transferred across borders does not fall within the definition of “personal data” then the legal requirements of the Safe Harbour and the Directive, including adequacy, do not apply.

Crucially there are different approaches in Europe and the United States - the United States have taken a much narrower approach to personal data. Data may activate one jurisdiction’s data protection law but not the other. This can raise compliance costs and cause substantial uncertainty for organisations operating across borders. Additionally the Article 29 Working Party (Art 29 WP), an advisory data protection body with a representative from each Member State, has noted a diversity of approaches to the scope of “personal data” across Member States, let alone between the United States and Europe.88

The line between personal and non-personal data has proved to be uncomfortably amorphous, creating substantial uncertainty. This occurs as emerging technologies can reidentify ostensibly “anonymised” or “non-personal” data in some circumstances. This has significant privacy implications as non-personal data does not engage the requirements of adequacy. Therefore governments and businesses can freely share and sell anonymised data yet specific individuals could still be reidentified and have their privacy violated.

1 United States Approach

The United States, with their sectoral approach to data protection, does not have a common definition of personal data. However there are three main approaches being: the tautological; the non-public; and the specific types approach. Having

multiple approaches to what constitutes personal data clearly increases the complexity of achieving adequacy.

The tautological approach lacks elegance and provides little guidance with self-referential descriptions. For example the Video Privacy Protection Act of 1988 defines personally identifiable information as “information which identifies a person.”\textsuperscript{89} Sifting out personal data from non-personal data is very difficult under this approach and whilst its open ended nature provides flexibility for new technologies, conclusions reached under the approach are likely be based on ad-hoc intuitions of judges and regulators.\textsuperscript{90}

The non-public approach, rather than defining personal information directly, simply excludes publicly accessible information or information that is purely statistical from being personal information. For example the Gramm-Leach-Bliley Act of 1999 defines “personally identifiable financial information” as “non-public personal information.”\textsuperscript{91} Here the issue is that the public/private divide is not the same as the identifiable/not identifiable divide. Publicly available information in connection with other publicly available information or in connection with non-public information can identify individuals in certain contexts but the data may not be subject to data protection law under this approach.\textsuperscript{92}

The specific types approach designates certain categories of data as per se personal information. For example under the Massachusetts data breach notification statute, personal information is someone’s first name and last name together, or first initial and last name combined with a social security number, credit/debit card number, driver’s license number or financial account number.\textsuperscript{93} Professor Daniel Solove

\textsuperscript{89} 18 USC § 2710(a)-(b).
\textsuperscript{93} Mass Code 201 § 17.04.
argues this approach suffers from rigidity in that data outside the categories could still reveal a lot about an individual, particularly in combination with other data.\textsuperscript{94}

\section*{2 Directive and the Regulation}

The Directive defines personal data as “information relating to an \emph{identified} or \emph{identifiable} natural person” \textsuperscript{95} (emphasis added). “Identified” is not defined in the Directive but member countries have interpreted the concept variously. For example in Germany a person is identified when “it is clear that the data relate to the person and not to another” and in the United Kingdom a person is identified if “there is sufficient information either to contact him or to recognise him by picking him out in some way from others and know who he/she is.”\textsuperscript{96}

The set of personal data is expanded significantly under EU law by the concept of an “identifiable” natural person. The Directive defines an “identifiable” person as “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”\textsuperscript{97} Further guidance is given by the note that “account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.”\textsuperscript{98} Information at the wider level of “identifiable” and the narrower “identified” are treated equally and subject to the full rights and duties of the Directive, including adequacy.

The Regulation maintains the concept of identifiable but shifts the nomenclature to “indirectly identified.”\textsuperscript{99} Personal data is defined as “any information relating to a data subject” and a data subject is anyone who can “be identified, directly or indirectly, by means reasonably likely to be used.” Furthermore the new technology

\textsuperscript{94}Schwartz and Solove, above n 92, at 1831.
\textsuperscript{95}Art 2(a).
\textsuperscript{96}Schwartz and Solove, above n 90, at 888.
\textsuperscript{97}Art 2(a).
\textsuperscript{98}Recital 26.
\textsuperscript{99}Art 4(1).
centric examples of location data, online identifiers and genetic identify are given as possible links that might directly or indirectly identify a person.

Professor Daniel Solove and Schwartz criticise the European approach on its lack of nuance- it does not distinguish between different levels of “identifiableness.” Some data with names, addresses, birth dates and social security numbers very clearly identify specific individuals. However other data relating only to an “identifiable” rather than “identified” individual require further effort to narrow the data down to a specific individual. The disparity in the effort and resources required to identify data at the lower end of the continuum of “identifiable” from data that have already been identified is not considered under the European approach- the law treats them the same. This can mean disproportionate compliance costs for data processors and controllers who are handling personal data with different levels of risk.100

Solove and Schwartz argue the “all means likely reasonably to be used” test is a strength of the European approach as it gives flexibility as new technologies are discovered.101 However I believe the test lacks perspective in some contexts. For example, a well-resourced and dedicated adversary might be able to reidentify personal information from anonymised data using means that would not be “likely reasonably to be used” under the test.

Turning personal data into non personal data through anonymisation has relieved legislatures of balancing privacy with the free flow of information. The risks of reidentification and subsequent privacy harm have been deemed incredibly low therefore the requirements of data protection law have not applied to anonymised data (emphasis added). Whilst this assumption of risk may have held truth in the past it is becoming far less accurate. Reidentification science is driven forward by two increasing factors- the power of computer hardware and the richness of

100 Schwartz and Solove, above n 90, at 887.
101 At 892.
auxiliary information.\footnote{102} Professor Paul Ohm describes the promise that anonymisation protects privacy as an ‘empty one.’\footnote{103}

Professor Arvind Narayanan and Professor Vitaly Schmatikov equate the medieval alchemists belief in turning lead into gold with the belief records containing sensitive data can be transformed into non personal data.\footnote{104} Reidentification science does not just show a flaw in a particular anonymising or pseudonymising technique, but shows the fundamental inadequacy of the entire paradigm of deidentifying data.\footnote{105} Nevertheless data is persistently sold and shared with a belief privacy will be protected through pseudonymisation and anonymisation.

For example in the mid-1990s a government agency in Massachusetts released every state employee’s medical records to researchers after removing explicit identifiers such as name, address and social security number. Privacy had been protected, assured the Governor. Graduate student Latanya Sweeney, after purchasing voting records and combining them with the medical records, reidentified the Governor’s records and promptly sent them to his office.\footnote{106} Paul Ohm predicts this generation’s computer scientists will shock with examples of seemingly implausible reidentification.

A particularly unsettling reidentification example concerns location data from cell phones. Cell phone location data can be incredibly useful for urban planning, emergency response development, business and epidemiology- however the anonymised location data of users has significant privacy implications. Unsettlingly researchers in Belgium and the Massachusetts Institute of Technology analysed 1,500,000 cell phone users over fifteen months and discovered just four location

\footnotesize{\footnote{102} Paul Ohm “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation” (2010) 57 UCLA L Rev 1701 at 1731.}  
\footnotesize{\footnote{103} At 1704.}  
\footnotesize{\footnote{105} At 26.}  
\footnotesize{\footnote{106} Ohm, above n 102, at 1720.}
points over a year, when combined with publicly available information such as twitter feeds, were enough to uniquely identify 95% of users.\textsuperscript{107}

Reidentification science is completely undermining the current approach to what constitutes personal data. This is a fundamental issue for data protection law and will be discussed further in section VIII(A)(3).

\textit{D Facebook}

“I want to meet Mark Zuckerberg one day and thank him….I’m talking on behalf of Egypt….This revolution started online. This revolution started on Facebook.”\textsuperscript{108}

“If Facebook were a government agency, its power would be as undisputed as it would be frightening…If a government department had so much up to the minute information about who we know, where we have been and what we are doing at its fingertips then one can only imagine the outcry.”\textsuperscript{109}

How can we reconcile these positions? The first statement from Wael Ghonim, a Google executive who helped catalyse the Egyptian revolution in 2011 captures the optimism of Facebook’s political value. The second, by Australian Writer Julian Lee, feeds anxieties of corporate and government power.

Facebook plays host to these complex issues and more: the power relationship between a state and its citizens; the balance of power between corporate and state actors; how the law restricts corporate and state action; how social norms concerning privacy shift over time; how to regulate algorithms; and the extent to which fundamental rights to privacy and data protection can be infringed in the interests of national security. These debates pervade a wider conversation about

\textsuperscript{107} Yves-Alexandre de Montjoye and others "Unique in the Crowd: The Privacy Bounds of Human Mobility" 2013 Scientific Reports 3(1376).
\textsuperscript{108} Anupam Chander "Facebookistan" (2012) 90(5) NC L Rev 1807 at 1834.
\textsuperscript{109} At 1813.
data protection in the modern era but are tethered to Facebook as an archetypal example.

Facebook is the world’s largest social networking website. Users share photos, messages and videos with each other and are subject to targeted advertisements based on their activity. Its mission is to change the world’s information architecture to a “network built from the bottom up...rather than the monolithic, top-down structure that has existed to date.”\textsuperscript{110} This invites a sense of empowerment, the unpicking of the status quo, a reclaiming of control over information flows. However the website’s architecture funnels the personal data of users up Facebook’s hierarchy who then on sell to advertisers or release the data to law enforcement.

From an economic perspective, Facebook greatly benefits from analysing its users’ personal data. Revenue increases are driven by ads targeted to users exhibiting specific behaviours or characteristics desired by the advertiser.\textsuperscript{111} “User” is employed in this setting as “customer” obscures the true business model. Clarity is gained by viewing the customers of Facebook as the advertisers with the users as the producers and the asset being traded as personal data. Beyond targeted advertising, Facebook is diversifying its e-commerce revenue streams with new features such as Marketplace, a buy, sell and exchange platform. In 2015 Facebook recorded total revenues of USD 17,930,000,000 which was an increase of 44 per cent on the prior year.\textsuperscript{112}

Facebook is the means by which an increasing number of individuals connect to each other and the world. In a recent Pew Research Centre survey more than 62 per cent of American adults stated they receive news from social networking sites,\textsuperscript{113} predominantly from Facebook with Twitter playing a lesser but important role. This is a profound shift of power from traditional media channels to social networks.

\textsuperscript{110} Ibid.
\textsuperscript{111} Alessandro Acquisti and Hal Varian “Conditioning Prices on Purchase History” (2005) 24(3) Marketing Science 1 at 15.
\textsuperscript{112} Facebook “Facebook Reports Fourth Quarter and Full Year 2015 Results” (26 January 2016) PR Newswire <www.prnewswire.com>.
Whilst other social networking sites such as BEBO and Google Plus have enjoyed pockets of success, Facebook has now achieved considerable market dominance.

Mark Zuckerberg, Chief Operating Officer and Founder of Facebook, encourages users to share more content with more people, declaring in 2010 that privacy is no longer a social norm. Facebook has attracted significant criticism for how they gather and treat the data of their users. For example they conducted, without consent, secret psychological tests on 700,000 users in 2012. The website changed the positivity or negativity of peoples’ newsfeeds - the content they see - to determine how users would respond. Chief Operating Officer Sheryl Sandberg refused to apologise for the lack of consent, instead apologising for how the tests were communicated.

In Europe the personal data of Facebook users are transferred to the United States for processing. It is this international transfer which engages the requirements of adequacy. Concern was raised by Max Schrems over whether this data flow was subject to mass surveillance after being transferred. Hogan J in the Irish High Court found the NSA did have considerable access to Facebook data, believing there was ‘no other realistic conclusion.’ Mark Zuckerberg however has denied Facebook is a conduit to mass surveillance and declared he had no knowledge of the PRISM surveillance program until after the issue received public ventilation.

Beyond the United States, other governments are well aware of the value of Facebook data, with the Chinese Academy of Social Sciences concluding the networking site was “exploited by Western intelligence services and used for subversive purposes... its special political function can be a threat.” However the website is utilised for the political purposes of citizens as well as their governments. For example prior to the Ben Ali dictatorship falling in Tunisia, Facebook was a

---

116 Schrems, at [24].
118 Dominic Rushe "Facebook and Google Insist They Did Not Know of Prism Surveillance Program" (8 June 2013) The Guardian <www.theguardian.com>.
119 Chander, above n 108, at 1831.
crucial platform for disseminating videos and information about the oppressive regime, giving a voice to isolated pockets of the Tunisian population. Activists such as Mohamed Bouazizi, who committed suicide by self-immolation in protest, were broadcast all over the world in Facebook videos. Conversely however, the Tunisian government was, at the same time, using JavaScript insertions to steal the Facebook passwords of activists in order to remove pages considered harmful to the government’s interests.

Facebook is a strong example of how modern business corporations can rival the power of states. With over a billion users only China and India can compete with Facebook’s “population.” Facebook also sends diplomats (lobbyists) to foreign countries with Mark Zuckerberg enjoying access to heads of state. Addressing the G8 in 2011 he argued excessive internet regulation would not work and more recently he was the guest speaker at the APEC leaders’ summit in Peru.

How content is delivered to users is determined algorithmically by factors such as friend relationships, explicitly expressed interests and content quality. These algorithms can hold considerable power over political opinions. Whilst there is the potential for social media to deliver a broad spectrum of political content, there is concern users exist in echo chambers and filter bubbles. These occur when algorithms, over time, create social media spheres in which users predominantly view content agreeable to their pre-existing preferences, insulated from conflicting viewpoints. This effect exists and is statistically significant however its exact magnitude is contested.

---

120 At 1813.
121 Ibid.
126 Eytan Bakshy, Solomon Messing and Lada Adamic "Exposure to Ideologically Diverse News and Opinion on Facebook" (2015) 348(6239) Science 1130 at 1130.
Algorithms produced by third parties using Facebook data are also of concern. For example Admiral, one of the largest car insurance companies in Britain, was forced to recall their initiative to set premiums from mining Facebook data. The company believed users writing concise sentences, using lists, not using exclamation marks, using measured language such as “maybe” rather than “always” or “never” and arranging catch ups at specific locations and times rather than just “tonight” were less likely to crash their cars. After a negative public response to the initiative Facebook decided to find Admiral as operating outside Facebook’s terms of service.

People continue to reveal traditionally private information on Facebook, be that sexual orientation, net worth, relationship status or political affiliation. These revelations can be consensual and explicit however further non-transparent processing of such data for secondary purposes can conflict with the Directive. As Big Data analytics continues to develop these issues of automatic processing and secondary uses of data will likely increase.

Facebook is critical to this thesis not just for how it catalysed the shaping of adequacy in Schrems but for its microcosm position in the general conversation on regulating emerging data technologies. Facebook was not the only corporation exposed in Snowden’s leaks however its market dominance and the extent and sensitivity of personal data circulating on the website make it an incredibly useful lens to view the requirements of adequacy through.

E Key Points:

Privacy is conceptualised in terms of personal dignity and personal autonomy in Europe. It is about enjoying a personal space in which to develop and grow.

Privacy is conceptualised in the United States as freedom from state intervention. It is about having dominion over one’s body or home.

---

However there are considerable economic and political factors shaping privacy. For example United States legislators appear more willing than European legislators to compromise privacy for an attempt at greater business efficiency and national security.

These divergent views have resulted in a considerable clash over how personal data should be protected and what personal data should be protected when it is transferred internationally. “Adequate protection” is the standard required by the EU.

The divergent views of the United States and EU characterise an incredibly tense data protection debate. Schrems increased tensions when the ECJ found the means by which the United States achieved adequacy, the Safe Harbour, to be invalid.

Facebook provides a useful lens to view adequacy as it can be seen as a microcosm of global data protection issues and was the subject of the Safe Harbour decision.
III INTRODUCTION TO ADEQUACY

Adequacy is a standard in EU data protection law which when achieved allows transborder data flows to occur. It is a tool to protect the personal data of those in the EU.

Under art 25(1) of the Directive, Member States can only transfer personal data to countries outside of the European Economic Area who ensure an adequate level of protection, unless certain specific derogations apply. This protects personal data from being transferred to a jurisdiction providing less protection. Europe could have impeccably high standards but the privacy of subjects could still be violated if one link in the processing chain was in a less protected domain.

The adequacy examination requires a case by case analysis “in light of all the circumstances surrounding a data transfer operation.” This suggests a granular inquiry of specific transfers, corporations or sectors, however the European Commission can find an entire country ensures adequate protection.

A country can ensure adequate protection by reason of its domestic law, professional rules and international instruments and is assessed under art 25(6) of the Directive for the “protection of the private lives and basic freedoms and rights of individuals” provided. The core fundamental rights referred to are the right to privacy and the right to protection of personal data.

Once a country has a positive adequacy decision transborder data flows between that country and the European Economic Area are presumed to be suitably protected. However before an adequacy decision is made by the European Commission, the Art 29 WP provides an opinion on the level of protection of personal data in the applicant country.

128 Art 25(2).
129 Ibid.
130 Art 25(6).
Whilst the Art 29 WP reports follow a set structure looking at specific data protection principles, they also take a wide look at the applicant country’s legal landscape and how that landscape might hinder or promote data protection. For example in New Zealand’s report, it was relevant that there is no written constitution in the traditional sense but higher law in the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993. So too was it relevant that New Zealand is a parliamentary democracy, with an independent Privacy Commissioner and independent judiciary with common law links to the United Kingdom. Even New Zealand’s business culture and small size where dissemination of poor data handling practices spread quickly were considered factors.\cite{131} The Art 29 WP opinions use the same data protection principles to structure the analysis however each report is a unique exploration of how the applicant compares to the European standard.

In EU law, Directives are legislative acts which set out a standard or goal for the law but allow individual Member States to implement their own laws to achieve that standard. This is in contrast to a Regulation which has direct binding force. The resulting flexibility inherent in implementing Directives allows Member States of the EU to express slight legal differences in their data protection. Crucially countries outside the EU applying for adequacy are also given flexibility in the implementation of the relatively high European standard. This flexibility plays a political role as declaring a country’s data protection standards as inadequate can be seen as a slight- flexibility can provide breathing space for countries with different methods of providing protection.

The EU has an interest in multiple countries achieving adequacy. This encourages trade with Member States, protects the privacy of European subjects and also propagates European privacy norms rather than United States norms. However successful applicants are often extended some flexibility. For example New Zealand was not without issue- the Art 29 WP stated New Zealand failed to fully comply with the direct marketing principle but it “did not believe there is a major shortfall or that this needs to stand in the way of an ‘adequacy’ finding.”\cite{132} Crucially the opinion

\footnote{131 Article 29 Working Party “Opinion 11/2011 on the level of protection of personal data in New Zealand” (00665/11/EN WP 182, Adopted 4 April 2011) at 13.} \footnote{132 At 11.}
stated, “although some concerns still exist, adequacy does not mean equivalence with the Directive”\textsuperscript{133} and hence a positive adequacy finding was recommended. Whilst adequacy is a legal standard, it is an instrument of diplomacy. This political component helps to explain why the meaning of adequacy is under stress, the political angle must be kept firmly in mind throughout this thesis. In New Zealand’s case, it appears the discretion was awarded in light of the “pioneering role” New Zealand is expected to play in developing data protection laws in the Pacific.\textsuperscript{134}

If a country fails to achieve a positive adequacy finding from the European Commission, or has not applied, there are other ad hoc mechanisms through art 26 which can allow for the transfer of data.

First, there is a list of narrow derogations, such as when the data subject has given his consent unambiguously to the proposed transfer or the transfer is required for the performance of a contract.

Second, a company can use Model Contractual Clauses (MCMs). Specific clauses have been approved by the European Commission and organisations can achieve adequate protection by subjecting themselves to them. Effectively they implement the principles of the Directive into off the shelf contracts allowing for rapid approval\textsuperscript{135}. Initially they were met with dissatisfaction however after being remodelled with greater input from the business community they have achieved greater prominence\textsuperscript{136}. The MCMs impose significant obligations on the data exporters. For data transfer to occur there must be a legal basis for processing in the recipient country and the data must have been collected and processed legally before being transferred\textsuperscript{137}.

\textsuperscript{133} At 15.
\textsuperscript{135} Schwartz and Solove, above n 27, at 1981.
\textsuperscript{137} At 200.
Thirdly, a company can subject itself to Binding Corporate Rules (BCRs). They are available for a company or group of companies transferring data across borders but within the company or group. Each Data Protection Authority in each country involved in the transfers must approve the BCRs before they are valid, making approval lengthy and expensive. Large corporations who have utilised BCRs include General Electric and Hewlett-Packard. It is worth noting BCRs and MCMs can be used in tandem. For example a corporation may use a BCR to transfer data internationally within a corporate group but use MCMs to transfer data internationally outside of that group.

The European Data Protection Authorities prefer full country adequacy decisions over BCRs and MCMs as a basis for transfer. This is because BCRs and MCMs only create small pockets of adequacy in a country with otherwise inadequate protection. The list of derogations are the least preferred and they are interpreted narrowly and strictly as they do not protect personal data once it has left the European Economic Area. The Data Protection Authorities are sceptical about allowing the exceptions to be used as a basis for transferring large volumes of data.

Finally, there is the specific case of the United States who negotiated the Safe Harbour. Whilst the United States has not received a formal finding of adequacy through the normal route, the Art 29 WP opined the United States did not provide adequate protection for personal data prior to Safe Harbour. The special scheme was activated in 2000 when the European Commission released the Safe Harbour Arrangement and supporting documents. It is a voluntary self-certification program for United States firms overseen by the Federal Trade Commission (FTC) whereby members agree to be bound by certain negotiated data protection principles in order to receive data from the EU.

139 Kuner, above n 136, at 158.
140 At 210.
142 Schwartz, above n 27, at 1981.
A What are the Adequacy Principles in the Directive

The adequacy principles are the foundation of European data protection. Under the Directive, adequacy analysis has two components - the content of the data protection rules and the effectiveness of their enforcement.

Whilst a holistic analysis is used, the core of adequacy is found in the extent the following principles and enforcement mechanisms are provided for by the laws of the applicant country. If the principles are contained in a country's legal system, and appropriate enforcement mechanisms are in place, adequacy will be satisfied.

The Art 29 WP has outlined the core data protection content principles as:

(i) purpose limitation;
(ii) data quality and proportionality;
(iii) transparency;
(iv) security;
(v) rights of access, rectification and opposition; and
(vi) restrictions on onwards transfers.

Additional areas of analysis for specific types of processing are:

(i) sensitive data;
(ii) direct marketing; and
(iii) automated individual decision making.

From a procedural and enforcement perspective, the analysis also looks at:

(i) the level of compliance;
(ii) the support and help to individual data subjects; and
(iii) redress mechanisms.\(^{143}\)

These three clusters of (i) core principles, (ii) specific processing requirements and (ii) procedural and enforcement considerations, provide the framework for adequacy analysis.


If an applicant country has introduced data protection legislation adopting the norms of the OECD guidelines, United Nations Guidelines or the Council of Europe Convention 108 their likelihood of satisfying adequacy is significantly improved.

The Council of Europe Convention in particular if ratified is a strong indicator of adequacy. Whilst it does not restrict onwards transfers to third countries it does contain the other five core content principles and also requires safeguards for the protecting of sensitive data.

1 Purpose limitation

The purpose limitation principle has two component: (i) data must only be processed for a specific purpose; and (ii) the data must not be used in a way incompatible with that purpose.

The purpose for processing must be explicitly specified prior to or at the time of collection. There is a strong push for the purpose to be in writing, improving transparency and allowing comparison with subsequent processing purposes.

The context of collection and the reasonable expectations of the data subjects largely

---

144 Convention 108, above n 38.
147 Article 29 Working Party “Opinion 03/2013 on purpose limitation” (00569/13/EN WP 203, Adopted 2 April 2013) at 15.
determine the detail required.\textsuperscript{148} Vague purposes such as “improving users’ experience” are unsatisfactory and larger companies using data analytics have to be more thorough in their purpose specification than smaller companies doing limited processing.

Collection is the first processing operation so any processing beyond that, including simple storage, must not be incompatible with the original purpose.\textsuperscript{149} The Art 29 WP believes the compatibility assessment to be one of the most difficult monitoring tasks in data protection as well as one of the most important - it is the substance of the relationship between the purpose for which the data were collected and the purpose for further processing which determines compatibility.\textsuperscript{150} Sometimes compatibility is obvious, for example if an online retailer selling weekly vegetables boxes collected the personal data of a customer, further processing for payment and delivery each week would be prima facie acceptable. However the transfer of the data to another business selling organic meat boxes each week would not.

The context of collection and the reasonable expectations of the data subjects are critical for substantively assessing incompatibility with a balance of power analysis also relevant. For example consider a receptionist found shirking her work duties by a security camera. If the cameras were installed for security purposes then under the purpose limitation, she could likely reasonably expect the footage gathered to be used solely for security purposes and not for employment termination decisions.\textsuperscript{151} Additionally if a data subject was obliged to provide the data under law or had their freedom of choice constrained, perhaps by being unable to easily terminate the relationship with the data controller, then the incompatibility assessment is stricter.\textsuperscript{152}

\textsuperscript{148} At 51.
\textsuperscript{149} At 21.
\textsuperscript{150} At 23.
\textsuperscript{151} At 56.
\textsuperscript{152} At 24.
2 Data quality and proportionality

Under the Directive data must be “adequate, relevant and not excessive” relating to the purposes for processing, and must be “accurate, and where necessary, kept up to date.”¹⁵³

To reduce excessive processing art 7 of the Directive provides that personal data may only be processed if certain factors are satisfied. The factors are consent, necessary for compliance with a legal obligation, necessary to protect the vital interests of the data subject, necessary for the performance of a task in the public interest or necessary for the purposes of the legitimate interests pursued by the controller. The breadth of factors appears to substantially widen the situations in which data may be legally processed however “necessary” acts here as a limiting valve on what processing may occur.

In contrast to the purpose limitation principle which operates at the point of collection to reduce excessive collection, data quality and proportionality can operate after processing has occurred as data must be “kept in a form which permits identification of data subjects for no longer than is necessary.”¹⁵⁴

For example perpetually holding DNA and fingerprint data of a data subject acquitted of the crime the data were gathered to solve, was found to be disproportionate in the United Kingdom. After considering the Directive and the Council of Europe Convention of 1981 the Court held the “blanket and indiscriminate nature of the powers of retention” were not proportionate to the legitimate goal of crime fighting.¹⁵⁵ Other countries in Europe were holding the data for two years under certain conditions whereas the United Kingdom wanted to hold the data indefinitely to build a large crime fighting database.

¹⁵³ Art 6(1)(c)-(d).
¹⁵⁴ Art 6(1)(e).
¹⁵⁵ S & Marper v United Kingdom [2008] ECHR 1581 at [125].
3 Transparency

The principle of transparency requires data subjects to be informed about who is processing their data\textsuperscript{156} and the purposes for which the data are being processed.\textsuperscript{157} Sunlight is said to be the best disinfectant, so too for data processing.\textsuperscript{158} Fairness demands data subjects are made aware of how and by whom their data is processed.

However a discord between transparency and understanding persists. A subject may be aware of the processing occurring but might not understand how the processing will affect their online profile. It is difficult to know how best to catalyse the higher value of understanding by providing transparency.

Art 10 of the Directive controls data gathered directly from a data subject whereas art 11 concerns indirect gathering and contains an additional provision whereby no information needs to be provided if it would prove impossible or would involve disproportionate effort.\textsuperscript{159}

Further information including the recipients of the data, what the rights of access and rectification are and whether the data supply is obligatory or voluntary have to be provided to data subjects. However it is only required “in so far as such information is necessary” in order to guarantee fair processing, having regard to the context of collection.\textsuperscript{160}

The burden this places on data controllers is unclear as it is difficult to know when the provision of this further information is necessary. On this point the Member States have shown considerable divergence in implementing the Directive. For example the United Kingdom requires information to be provided only “insofar as practicable.” Adopting a stricter approach for when the data has not been gathered

\textsuperscript{156} Art 10(a) and 11(1)(a).
\textsuperscript{157} Art 10(b) and 11(1)(b).
\textsuperscript{158} Quote is attributed to Louis Brandeis, a highly influential privacy scholar and judge from the United States.
\textsuperscript{159} Art 11(2).
\textsuperscript{160} Art 10(c) and 11(1)(c).
directly from the data subject, Italy necessitates the providing of further information in writing, irrespective of the necessity test.\textsuperscript{161}

4 Security

The security principle requires that technical and organisation measures, appropriate to the risks, are taken by the data controller when processing data. This includes making sure anyone acting under the data controller’s authority does not process data except as instructed by the controller. The security principle is expressed through art 16 of the Directive requiring confidentiality and art 17 requiring security of processing. There is a general obligation of the result of security of processing without the requirements of specific measures to achieve that result. Whilst some Member States, such as Spain, have detailed regulations of what technical and organisational measures should be taken, none of the countries receiving adequacy decisions has done so.

Art 17 requires, regarding the ’state of the art,’ implementation costs, the risks of processing and the nature of the data, that appropriate technical and organisational security measures are taken. However identifying and responding to different risks can be an incredibly technical and nuanced requirement- whilst many organisations and countries have dealt with financial risk and legal risk from breach of confidence, dealing with cyber-security risk is a relatively new field. Specialised knowledge is required to understand how data security may be threatened in different settings, making the security principle particularly perplexing for the data subject and lawyer alike.

5 Rights of access, rectification and opposition

Under this principle data subjects should be able to obtain a full copy of their personal data and rectify the personal data when incorrect. Additionally they should be able to object to processing in certain contexts. This principle is about allowing data subjects to participate in, and have some level of control over, the processing

\textsuperscript{161} Douwe Korff “Analysis and impact study on the implementation of Directive EC 95/46 in Member States” (Report for European Commission, University of Essex, 2002) at 19.
of their data. To the extent this can be achieved, this principle is crucial to informational self-determination.

Under art 12(a) data subjects have the right to obtain, without constraint and excessive delays or costs: information as to whether their data are being processed; the purpose of processing; and the logic involved in automatic processing. Art 12 also provides for the rectification and erasure of incomplete and inaccurate data.\footnote{Art 12(b).}

Under art 14(a) data subjects have the right to object to data processing generally with art 14(b) giving the specific right to object to direct marketing.

It is important to note how principles can be interdependent. For example the transparency principle and the purpose limitation principle with their notification requirements contribute significantly to the exercise of access, rectification and opposition rights—without an awareness of what data processing is occurring, it would be difficult to object to that processing.

6 Restrictions on onward transfers

Transfers of personal data beyond the transborder flow are only allowed when the second recipient also provides an adequate level of protection. This is needed as otherwise the Directive could be circumvented by transferring data out of the EU’s jurisdiction. The only permitted exceptions are those found in art 26(1) of the Directive which include the data subject unambiguously consenting to the proposed transfer or the transfer being required for the performance of a contract.

7 Sensitive data

The Directive outlines that certain categories require extra protection and special rules for processing. The sensitive categories of data are listed in art 8 of the Directive, being personal data revealing: racial origin; ethnic origin; political
opinion; religious or philosophical beliefs; trade-union membership; health data and data concerning sex life.

However what constitutes sensitive data can shift depending on the context. For example someone’s food preference on a flight might not reveal sensitive data but equally it could reveal health information if the data subject had specific dietary requirements and could also reveal religious information if the data subject required a halal meal. Nevertheless the Directive takes a categorical approach where certain categories of data are held to a higher standard.

8 Direct marketing

Under this principle, data subjects should be able to ‘opt out’ of having their data transferred for the purposes of direct marketing. The general right to object to processing is found in art 14(a) with 14(b) specifically addressing direct marketing. Every Member state with the exception of Luxembourg has adopted a ‘Mailing Preference List’ or ‘Robinson List’ which allows data subjects to opt out of receiving direct marketing. The implementation of this principle is noteworthy for highlighting the role industry based codes of conduct can play in securing positive adequacy findings.

9 Automated individual decision making

Interestingly art 15(1) allows a data subject to object to automated decisions. This was innovative at the time of the Directive’s creation and some considered it to create a new principle- decisions which can substantially impact a person’s interests should not be fully automated. However art 15(1) only concerns decisions “based solely on automated processing.” This allows decisions made substantially by automatic means as long as a human is involved in some capacity at some stage.

163 Korff, above n 161, at 22.
164 Bygrave, above n 39, at 2.
As an increasing range of decisions are made by automated means this principle is likely to come under considerable stress in the future.

10 Procedural and enforcement mechanisms

Data protection systems require a good level of compliance with the rules, support and help to individual data subjects looking to exercise their rights, and appropriate redress to injured parties when rules are broken. This usually requires an independent data protection supervisor or privacy commissioner. Crucially this section includes a broad analysis of the accessibility and efficacy of a legal system.

If data subjects are prevented from enforcing their rights, it will be little consolation they have them in the first place.

B Discretion in Assessing Compatibility with Principles

Schrems found the European Commission’s discretion to be strict when deciding whether a country satisfies adequacy, due to the importance of data protection and the large number of data subjects whose rights can be infringed by inadequate protection. However this assertion betrays reality - the European Commission has exercised significant discretion in awarding adequacy decisions.

The Art 29 WP found New Zealand to have several weaknesses - with the most concerning being the lack of restrictions on onward transfers to other countries. The weaknesses were held to be mitigated by New Zealand’s size, geographical isolation and the small probability that significant volumes of personal data would be on transferred. The awarding of adequacy to New Zealand by the European Commission shows considerable discretion. It would be illuminating to know whether such discretion would still be offered if, irrespective of geographic isolation and limited data transferring, New Zealand had a politically caustic relationship with the EU.

165 At [78].
166 Article 29 Working Party, above n 131, at 10.
It is difficult to unpick the motivations behind such shifting tolerances of imperfections. Clearly there is a realpolitik component. A negative decision is an outcome the European Commission wants to avoid or at least hide - they do not want to discourage applicants and the scheme increases in value as more countries achieve adequacy. Nevertheless by hiding how discretion is exercised transparency is reduced. Indeed the Art 29 WP has never published a negative adequacy opinion, with the only examples of failed applications coming from external consultants.\footnote{Christopher Wolf “Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers” (2013) 43 Washington University Journal of Law & Policy 227 at 239.} Exercising discretion to overlook imperfections mitigates political embarrassment but without transparency it is impossible to see how the discretion is exercised on a case by case basis. Additionally negative decisions could be a useful resource for applicant countries looking to align their data protection with the standard of adequacy, even if the deeper motivations for the discretion remained hidden. In borderline cases knowing what is not up to the adequacy standard could be just as useful as knowing what is.

Without greater transparency it is incredibly difficult to know why certain countries adequacy decisions are blocked or encouraged. However there is some evidence of questionable concerns playing a role. For example Ireland delayed and officially objected to Israel receiving a positive adequacy decision from the European Commission. Initially dressed as concern over minor features of how manual data processing was carried out, Ireland later admitted to objecting in outrage over the alleged use of Irish passports by Israeli agents involved in targeted killing.\footnote{At 242.}

Ultimately the discretion exercised by the European Commission has caused uncertainty over the meaning and requirements of the adequacy principles. For example regarding Argentina’s application, the Art 29 WP was concerned the Argentinian Data Protection Authority lacked jurisdiction over all data processors and controllers in the state. Moreover there was no guarantee the Data Protection Authority would be independent, enforcement mechanisms were unclear and almost no enforcement was actually occurring.\footnote{At 241.} Nevertheless a positive adequacy
decision was made. This is a pointed difference to the position taken in *Schrems* where independence of supervisory authorities and access to legal redress were crucial underpinnings of adequate protection. Interestingly, members of the Art 29 WP have admitted “politics” entered into the decision.\textsuperscript{170}

**C Key Points:**

Adequacy is a standard of data protection countries outside of the European Economic Area must reach in order to process data originating in the European Economic Area.

It is a complex legal standard composed of core principles but also incorporates a wide analysis of the legal landscape in a third country.

Whilst the Art 29 WP follows a set structure of analysis applications are considered on a unique case by case basis.

However the amount of discretion afforded to different applicants varies. This makes it difficult to have a stable view of exactly what the requirements of adequacy are.

Crucially negative adequacy decisions are not published preventing a closer examination of the adequacy threshold.

\textsuperscript{170} Kuner, above n 3, at 66.
IV HOW WAS ADEQUACY SHAPED BY THE SAFE HARBOUR AGREEMENT?

The Safe Harbour agreement was found to provide adequate protection, before being invalidated in *Schrems*. By examining the level of protection provided it is possible to examine the threshold for adequacy.

A What Was the Safe Harbour?

Shortly after the Directive entered into force, tension surfaced between the United States and the EU over transborder data flows. The United States Government claimed restrictions on data flows threatened over USD 100,000,000,000 in trade. The Safe Harbour was the political and legal solution to the United States being highly unlikely to satisfy adequacy through the usual route.

The Safe Harbour was a voluntary data protection regime whereby United States organisations could self-certify they were complying with the Safe Harbour privacy principles, being: notice (subjects should be informed about how data is collected and used); choice (consumers must be able to opt out); onward transfer (transfers to third parties are only allowed if the third party provides adequate protection); security (should prevent loss of personal information); data integrity (data should be relevant and accurate); access (individuals should be able to access and correct their data); and enforcement (there should be effective means of enforcing the rules). It was a special route to adequacy outside of the usual country wide adequacy findings, Model Contract Clauses and Binding Corporate Rules.

The FTC enforced the scheme. If an organisation engaged in commerce made a public declaration to adhere to the Safe Harbour principles then failing to follow the principles could be deceptive practice under s5 of the FTC Act.

---

171 Bygrave, above n 1, at 194.
172 Safe Harbour, above n 56, at 4-6.
173 Jan Dhont and others “Safe Harbour Decision Implementation Study” (Report for European Commission, Namur, 19 April 2004) at 15.
The United States did not receive a normal finding of adequacy, indeed prior to the Safe Harbour decision the Art 29 WP believed the United States did not provide adequate protection.\textsuperscript{174} As discussed in the literature review, the United States conceptualises privacy differently to the EU- the United States have narrow constitutional privacy protections against state actors, a patchwork of federal statutes and limited privacy legislation at the state level.\textsuperscript{175} There was also scepticism of the European approach from the United States perspective, with Professor Lillian BeVier suggesting omnibus legislation and a centralised data protection board was “a little like recommending that the fox, albeit dressed up as a benign and friendly farmer, guard the chickens.”\textsuperscript{176}

The clash of ideology played out over two years of negotiation between the European Commission and the United States Department of Commerce. The European Commission consequently adopted Decision 520/2000/EC\textsuperscript{177} in 2000 recognising the Safe Harbour as providing adequate protection. This power was exercised by virtue of art 25(6) of the Directive. The final agreement was the result of considerable compromise.

An example of a compromise which reduced the protection afforded by the Safe Harbour was the exclusion of financial data. Corporate data rights are seen as crucial underpinnings to intellectual property and commerce- The United States did not want to cede any control of these data flows.\textsuperscript{178} There was a narrative in the United States that overzealous data regulation of the financial services could push corporations to do business elsewhere. The Department of Commerce resisted the Directive’s reach by claiming the Financial Modernisation Act of 1999 (GLB Act) imposed a level of data protection higher than most data protection laws in Europe.\textsuperscript{179} However the European Safe Harbour negotiators were sceptical as the GLB Act allowed for mergers across financial services which could result in data being transferred between affiliates and processed without the consent of the data

\textsuperscript{174} Article 29 Working Party, above n 141, at 2.
\textsuperscript{176} At 74.
\textsuperscript{177} Safe Harbour, above n 56, at 7.
\textsuperscript{178} Frasher, above n 9, at 789.
\textsuperscript{179} At 790.
subject. Additionally there were no consumer rights to access financial data and multiple agencies were responsible for enforcement depending on the corporate structure of the financial institution. Ultimately the success of the United States negotiators in excluding financial data considerably narrowed the amount of data that could flow through the Safe Harbour, reducing its effectiveness.

Two European Commission Staff Working Papers initially reported on the Safe Harbour’s implementation, the first in 2002, the second in 2004. The 2002 report noted the number of self-certifying companies was lower than expected, being only 129 at the time, however the scheme was described as getting off to a “relatively trouble free start.” Several weaknesses were identified, if not fully quantified, and described as teething problems. Substantial resources were used by the Department of Commerce to host seminars and workshops for interested organisations. Unacceptably, fewer than half of the organisations involved in the scheme were found to have privacy policies with all seven of the Safe Harbour principles. The 2004 report again showed the number of participants in the scheme was lower than expected and was described as cause for disappointment. Only 400 organisations had self-certified by the end of 2003 and fewer signed up in 2003 than in 2002. The low number of participants suggests the scheme was not widely viewed as overly beneficial. The surprise at the low number of participants suggests the European Commission Staff valued the scheme higher than the organisations considering membership.

B Substantive Protections

The principles of the Safe Harbour were different than those in the Directive.

The Safe Harbour principles were:
(1) notice, data subjects had to be informed their data was being collected and

---

180 At 791.
182 Ibid.
used and given contact information should they have inquiries;
(2) choice, data subjects had to be able to opt out of the collection and transfer of their personal data to third parties;
(3) onward transfer, transfers to third parties were only allowed if the receiving party provided adequate protection;
(4) security, reasonable efforts had to be made to prevent loss of collected information;
(5) data integrity, data had to be reliable and relevant for the purpose it was collected;
(6) access, data subjects had to be able to access their personal data and correct or delete it when inaccurate; and
(7) enforcement, there had to be effective means of enforcing these rules.

Whilst the nomenclature shifted the standard of protection was still required to be adequate. However several concerns became apparent before Schrems. As the language employed shifted, so too did the protection.

1 Data quality

The Safe Harbour regime looked to protect data quality through its principles of data integrity and access. Specifically they contained the concepts of purpose limitation, accuracy, completeness and compatibility of purpose. However the purpose limitation in the Safe Harbour was a husk of the principle in the Directive- it did not require the purpose to be explicit, specified and legitimate, nor were the requirements of fairness and lawfulness present. Also lacking was the requirement for data processing to be not excessive. Without those narrowing constraints on processing, the scope for further “compatible” processing was greatly increased, weakening data minimisation and reducing protection. This is particularly significant as data quality weaknesses, such as vague processing purposes, can compound by weakening other principles such as transparency.

183 At 10.
2 Legitimate processing

Under art 7 of the Directive processing is prohibited unless specific circumstances are satisfied such as unambiguous consent. The other five avenues under art 7 only allow processing if it is “necessary” for specified reasons—supporting a narrow approach for interpreting the exceptions.\textsuperscript{184} This is in contrast to the Safe Harbour which gave general permission for processing provided notice (informing data subjects of the purpose their data were being processed for) and choice (giving the data subject the opportunity to opt out from data processing) were satisfied.

The notice requirement was not particularly strenuous for United States organisations. Notice was to be provided when data subjects were first asked to provide data however the Safe Harbour allowed them to do so “as soon thereafter as is practicable”- this created space for misuse. The practicable allowance was removed when the processing was for a new purpose or for disclosing data to a third party. Nevertheless in light of the lack of purpose specificity discussed above data controllers could circumvent this requirement if the original purpose was sufficiently broad to include the “new” purpose. Crucially third party disclosure under United States law, for example law enforcement requests for data, could also override the notice requirements.

Additionally the choice component suffered the weakness of being opt out rather than opt in. The data subject was supposed to be “provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.”\textsuperscript{185} However data subjects may have simply missed the option to opt out- the passive Safe Harbour standard is lower than the active, unambiguous consent required in the Directive.

3 Onward transfer

Notice and choice were expected to provide suitable protection against onwards transfers of data under the Safe Harbour as the data subject had to be able to opt out

\textsuperscript{184} At 13.
\textsuperscript{185} Ibid.
of the onward transfer. This suggests the data subject was involved before every transfer of their data.

In comparison to the apparent case by case approach of the Safe Harbour, the Directive gives general permission for data transfers outside of the European Economic Area provided the recipient provides adequate protection. Superficially this suggests the Safe Harbour may have provided better protection against onward transfers as the data subject can opt out for each specific transfer. However I would caution against this position. First, United States law could override the Safe Harbour allowing transfers to take place irrespective of data subject consent. For example when law enforcement made a request for data access as part of an investigation. Second, if a data subject passively “agreed” to a privacy policy by ticking a box allowing for the onward transfer of data, well before such data was to be transferred, that weak consent (in the sense that it might not be informed, specific and unambiguous) could pre-empt the right to opt out.\footnote{186 At 15.}

4 Rights of data subjects

Rights of access, deletion, correction and amendment were contained in Annex I in the Safe Harbour with Annex II providing significant limitations. Under Annex II the right to access was “subject to the principle of proportionality or reasonableness” and if the information requested was neither sensitive nor used in decisions significantly affecting the individual then access rights could be limited to data that was readily available or inexpensive to provide.\footnote{187 Safe Harbour, above n 56, at 11.} This gives organisations room to deny legitimate access with any counterarguments having to go through a time consuming dispute resolution mechanism- many data subjects simply would not bother. The Safe Harbour organisation could also charge a “not excessive” amount for data access and were required to provide an answer only “without excessive delay and within a reasonable time period.” This allowed organisations to slow down the process of achieving access, perhaps hoping the data subject would become increasingly apathetic as time and costs increased.
Further access restrictions existed for confidential commercial information and instances where access was likely to “interfere with the safeguarding of important countervailing public interests.” It is unclear exactly what constitutes important countervailing public interests however national security, defence and public security were named in the Annex II.\textsuperscript{188} Certainly it would be difficult for a data subject to argue their access would not infringe confidential commercial information.

Disappointingly the right to deletion of data under the Safe Harbour scheme was limited to inaccurate data. This would deny a data subject the ability to request deletion of accurate data that had been wrongly collected or processed.\textsuperscript{189} Deletion of accurate data could occur through a dispute resolution mechanism requiring deletion as a sanction for unlawful processing however again this could be a considerable time and cost burden on the data subject.

5 Independence

The Safe Harbour was a self-certification regime with alternative dispute resolution providers and the FTC overseeing enforcement. Organisations provided a signed letter to the Department of Commerce with contact details, a statement they were binding themselves to the Safe Harbour, a description of the processing operations and a description of the privacy policy and where it could be found in full.\textsuperscript{190} An organisation could receive an external compliance review of whether their privacy policy was sufficient and whether it had been effectively implemented, but this was not mandatory, they could simply assess themselves. This placed a substantial amount of trust in the private sector. Professor Lillian BeVier stated having a central European Data Protection Board was like having a fox guard the chickens- perhaps the simile resonates more effectively in the context of self-certification through Safe Harbour.

\textsuperscript{188} At 12.
\textsuperscript{189} At 6.
\textsuperscript{190} At 9.
Certainly self-certification sits uncomfortably with the European Jurisprudence holding “complete independence” of national supervisory authorities as an “essential component” of protecting personal data.\(^{191}\) The supervisory authorities in Europe are described as “guardians of...fundamental rights and freedoms” by the Court of Justice.\(^{192}\) This is a high standard to measure the Safe Harbour against.

**C Preliminary Conclusions on the Safe Harbour**

In conclusion the Safe Harbour had systematic weaknesses which were well known prior to *Schrems*. The push for adequacy is a push for the widespread acceptance of a high water mark for data protection that respects fundamental rights. That the main trading partner of the EU opted for a special, lower protection, different approach is antithetical to the European intent to propagate a clear, high data protection standard of adequacy. David Flaherty, an ex United States British Columbia Data Protection Commissioner, noted the negotiations were an opportunity to pressure the United States into adopting European norms.\(^{193}\) They borrowed some of the language but the underlying protection was significantly compromised.

Ultimately the Safe Harbour showed the extent to which political and economic pressures can act against legal standards. Compromise is the currency of international bargaining but the adequate protection in the Safe Harbour is significantly below that required by the Directive- consequently adequacy as a high water mark must be seen as withering with the Safe Harbour.

\(^{191}\) Case C-288/12 *European Commission v Hungary* (CJEU 8 April 2014) at [2].
\(^{192}\) Case C-518/07 *European Commission v Germany* [2010] ECR I-1885 at [23].
\(^{193}\) Cate, above n 175, at 75.
V INTRODUCTION TO SCHREMS

A Who is Max Schrems and What Action Did He Take against Facebook?

Max Schrems is an Austrian lawyer and privacy activist. During a semester aboard at Santa Clara University in California, Facebook's privacy lawyer Ed Palmieri spoke to his class. Schrems was deeply unsettled by what he perceived as Palmieri’s limited grasp of European data protection standards.194

After completing a research paper on Facebook’s alleged misunderstanding of European privacy law, Schrems exercised his right of access and requested all the data Facebook held about him. He received a file more than 1200 pages long with information much more detailed than he expected, including messages he thought had been deleted.195

After receiving his personal dossier from Facebook, Schrems brought several complaints against Facebook Ireland Ltd (Facebook is incorporated in Ireland for tax purposes.) In August and September in 2011 the following were included in complaints laid with the Irish Data Protection Commissioner:

(i) “pokes” (application which notifies the ‘poked’ user) were kept after the user removes them;
(ii) shadow profiles were created for non-users;
(iii) users were tagged in photos without their consent, they have to opt out rather than opt in;
(iv) deleted posts were still kept by Facebook;
(v) messages were stored even after deletion;
(vi) the privacy policy was vague and unclear which impacted the legitimacy of consent;
(vii) facial recognition features were disproportionate and opt out rather than opt in;

195 Ibid.
(viii) many categories of data were not accessible (such as biometric face print);
(ix) Facebook failed to guarantee any level of data security;
(x) deleted friends were stored by Facebook;
(xi) the like button embedded on other websites tracked users all over the internet; and
(xii) users could be placed in groups without their consent.196

After three years of difficult engagement with the Irish Data Protection Commissioner all 22 complaints were withdrawn. The decision to withdraw was made in light of the Irish Data Protection Commissioner refusing to make a formal decision on the complaints, the Commissioner denying Schrems access to counter arguments made by Facebook and the rising financial and time costs of continuing to pursue the complaints.197

Schrems had considerable difficulty, in addition to the institutional inertia at the Irish Data Protection Commission, of financing the legal work and recruiting top legal talent, with many data protection lawyers unwilling to work against a large data processing corporation. In response, Schrems created the non-governmental organisation Europe-v-Facebook.org and accepted crowd funding for his campaign. The organisation’s central focus is whether European Data protection laws are enforceable in practice. Key areas of concern are: transparency; opting in instead of opting out; individual control of data; data minimisation; and open social networks. Just as people on different telecommunications networks can talk to each other, Europe-v-Facebook.org believes social networks should be opened so people can use other social media sites but still interact with people on Facebook.198

_Schrems_ was decided narrowly but should be contextualised against the wider goals of Europe-v-Facebook. They represent an important push for higher standards of data protection- a grassroots attempt to strengthen the meaning of adequacy in favour of data subjects. They currently have a privacy class action suit against

---

197 Ibid.
Facebook which they are looking to bring in the European Court of Justice as well as actions in Ireland, Belgium and Germany questioning the validity of the MCMs used as a backup by Facebook to transfer data. The class action has received considerable support with over 25,000 supporters signing up in a short amount of time with some further 50,000 registered to join the action if allowed.\textsuperscript{199} It is uplifting that a young lawyer and his peers have made such an impact on the shaping of adequacy. However given the widespread awareness of mass surveillance it is disappointing governments and other well-funded organisations left the responsibility to an underfunded student.

In spite of the resource constraints facing Europe-v-Facebook, a 23\textsuperscript{rd} complaint was made and pursued, concerning the forwarding of Facebook data from Facebook Ireland to the NSA via Facebook America. Facebook Ireland is within the Directive’s scope so the export of data is permissible only if there is adequate protection.\textsuperscript{200} It was this surviving complaint which led to the case of \textit{Schrems}.

On the 25\textsuperscript{th} of June 2013 Schrems complained to the Irish Data Protection Commissioner that his data was being sent from Facebook Ireland Ltd to Facebook Inc in the United States through the Safe Harbour scheme and that this scheme was not providing adequate protection. Of concern was Edward Snowden’s revelations that the NSA in the United States was being granted mass access to Facebook data under PRISM.\textsuperscript{201}

Schrems argued the purpose limitation expressed in art 6(1)(b) of the Directive was violated, relying on the Art 29 WP’s opinion that mass use of commercial data for investigative purposes is a breach of the fundamental right to privacy.\textsuperscript{202} Schrems also argued the principle of proportionality enshrined in art 6(1)(c) was violated as

\textsuperscript{199} Natasha Lomas “European Facebook Privacy Lawsuit Heads To Court In Vienna” (9 April 2015) TechCrunch <https://techcrunch.com>.
\textsuperscript{200} Ibid.
\textsuperscript{201} Max Schrems, above n 196.
during terrorism investigations, only “specific individualised data should be transferred...on a case by case basis.”

The Irish Data Protection Commissioner argued he had no duty to investigate what he described as a frivolous and vexatious complaint. However Schrems sought judicial review of the decision arguing failing to investigate the complaint and make a formal decision was unlawful. He successfully argued the Data Protection Commissioner could not rely on the Safe Harbour to dismiss his complaint as the complaint brought the validity of the Safe Harbour into question and draws on facts of mass surveillance that were unknown when the Safe Harbour began.

B Interlocutory Judgment of the Irish High Court

1 General remarks:

The narrowness of the legal issues decided betray the case’s complexity.

Whilst Hogan J endeavoured to “apply neutrally the applicable legal materials” he felt a “via media” between the United States and the EU could in many respects only be determined at “the level of international diplomacy and realpolitik.” He was clearly aware of the hegemonic component to mass surveillance, as he noted it was contributing to the “preservation and reinforcing of American global political and economic power.”

Justice Hogan showed support for surveillance however, declaring “these surveillance programmes have undoubtedly saved many lives and have helped to ensure a high level of security, both throughout the Western world and elsewhere.” He also declared terrorist attacks such as 9/11 and the London and Madrid train bombings, highlighted why “intelligence services needed as a matter of practical necessity to have access to global telecommunications systems in order to disrupt

---

203 At 15.
204 Maximillian Schrems, above n 117, at [63], [69].
205 At [4].
206 At [5].
the planning of such attacks." I caution against framing the benefits as obviously true and implying the attacks could have been prevented if only the current NSA mass surveillance tools were in use. I adopt a similar position to computer scientist Jarod Lanier- he believes a rational conversation on mass surveillance is prevented by the overestimation of the presumed benefits of supercomputing and big data analysis tools. This over optimism of mass surveillance tools masks the disconnect between the modelling and the underlying structure of reality. Indeed Lanier argues for more scientific analysis of the assumed security benefits, which would allow a more nuanced comparison against the very real privacy harms.

Additionally Hogan J believed Snowden’s disclosures may have put the lives of security operatives at risk and certainly hampered entirely legitimate counter-terrorism operations. Again this is a contested conclusion. Glen Greenwald and the other journalists given Snowden’s documents vetted the documents released to mitigate harm to United States individuals. Whilst the United States House of Representatives in their Executive Summary on Snowden’s leaks state Snowden “caused tremendous damage to national security” they do not provide any evidence of this damage in the report. Instead there is an assertion the “full scope of the damage is unknown” and that the United States Government will have to spend billions mitigating it. The United States government believes revealing the specifics of harms caused would present a further risk. Disappointingly Hogan J does not address these tensions.

Nevertheless Hogan J was supportive of Edward Snowden overall, finding his revelations “demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary

207 At [5] and [63].
209 Maximilian Schrems at [6].
211 At 2.
citizens.”\textsuperscript{212} It is just difficult to balance this statement with the assertion that \textit{entirely legitimate} counter terrorism operations were hampered (emphasis added).

Transparency in particular concerned him with the Foreign Intelligence Surveillance Court (FISC) criticised for its secret and \textit{ex parte} hearings. Additionally he was dismayed at the gag order preventing telecommunication companies from revealing the mass, undifferentiated hand over of records to the NSA.

Crucially he did find the NSA to have the ability to access Facebook data in the course of mass and indiscriminate surveillance, indeed he believed there was “no other realistic conclusion.”\textsuperscript{213}

2 \textbf{Issue of frivolity:}

Considerable attention in the judgment concerned the initial position that Schrems’ complaint was frivolous. Given the profound importance of mass surveillance and mass privacy invasion, that Schrems complaint could be frivolous rightly infuriated many. However the term does not just mean silly or futile, but incorporates “unsustainable in law” as a meaning.\textsuperscript{214} The Data Protection Commissioner felt bound by the Safe Harbour decision from investigating Schrems claim hence believed the request to be unsustainable in law rather than silly, foolish, or trivial.

3 \textbf{What was referred to the Court of Justice?}

Justice Hogan reworked Schrems’ complaint in an unusual judicial move. He believed the manner in which the Commissioner had interpreted and applied the Safe Harbour in light of the Charter was not the true objection. Rather Schrems’ complaint concerned the terms of the Safe Harbour regime itself- although he stressed the validity of the Safe Harbour had not directly been challenged in the proceedings.\textsuperscript{215}

\textsuperscript{212} \textit{Maximillian Schrems} at [8].
\textsuperscript{213} At [13].
\textsuperscript{214} \textit{Novak v Data Protection Commissioner} [2012] IEHC 449 at [39].
\textsuperscript{215} \textit{Maximillian Schrems} at [69].
Snowden’s revelations in conjunction with the entry into force of art 8 of the Charter suggested to Hogan J that a re-evaluation of the interpretation of both the Safe Harbour and the Directive might be necessary. 216 He was swayed by the general novelty and practical importance of mass surveillance issues for all twenty eight Member States of the EU and hence referred the matter to the European Court of Justice.

The issues he referred were:

(i) Whether a National Supervisory Authority is prevented from examining a complaint that data transferred to another country is not adequately protected, if a European Commission decision states that it is adequately protected; and

(ii) Whether the Safe Harbour is valid.

The first question investigates the extent to which supervisory mechanisms must be independent to provide adequate protection. The second investigates the extent to which the Safe Harbour itself provides adequate protection.

---

216 At [67].
VI SCHREMS IN THE EUROPEAN COURT OF JUSTICE

Schrems invalidated the Safe Harbour agreement and outlined a positive adequacy finding requires a level of protection not identical but “essentially equivalent” to that guaranteed in the EU under the Directive, in light of the fundamental rights in the Charter. 217 This is a clear divergence from the 2011 position of the Art 29 WP in New Zealand’s adequacy opinion where adequacy was found to “not mean equivalence with the Directive.”218

The new test gives discretion in the legal means of achievement, particularly in light of common, civil and federal law systems interacting, however the discretion in the final essentially equivalent level of protection required is held to be strict.219

In cases raising difficult or novel areas of law in the EU, Advocate Generals analyse the submissions made to the ECJ and deliver impartial non-binding opinions on legal solutions. Yves Bot was the advocate general in Schrems and his opinion shared considerable similarity to the conclusions reached in the Court’s final judgment. His reasoning is spread throughout my analysis.

Whilst from a simple semantic perspective adequacy implies satisfactory or sufficient protection of fundamental rights, Bot believed adequacy should be interpreted in light of the objective of a “high level of protection of fundamental rights.”220 This lead him to declare a third country can only achieve adequate protection when it offers a level of protection “essentially equivalent” to the protection afforded by the Directive.221 This terminology and high standard of protection was adopted in the ECJ and is the current standard for achieving adequacy.

---

217 Schrems at [73].
218 Article 29 Working Party, above n 131, at 15.
219 Schrems at [74] and [78].
221 At [141].
“Essentially equivalent” is an artful term, providing more flexibility than identical whilst still demanding a high standard of protection - it appears to go to the substance rather than the form of the protection provided. Although crucially the ECJ does not specifically define essentially equivalent nor is there an examination of what the EU baseline is.

These incredibly vital but broad questions are left wanting by the judgment, with instead a narrow focus on (i) the powers of national supervisory authorities in the EU and (ii) whether the Safe Harbour is valid.

Before examining the case it is important to be precise about what the ECJ judgment held concerning the validity of the Safe Harbour. Art 1 of the Safe Harbour was found invalid for not duly stating the reasons the Safe Harbour ensured adequate protection, and art 3 was found invalid for restricting the National Supervisory Authorities. As the articles were inseparable from the rest of the decision, the entire scheme was found to be invalid.222

The Court did not undertake an analysis of whether or not the United States provides an adequate level of protection. Nor did the Court specifically decide whether the Safe Harbour framework provided an adequate level of protection. Instead, the Court found the powers of the National Supervisory Authorities were unlawfully restricted and the Commission decision approving the Safe Harbour failed to engage in a thorough enough analysis under the requirements of EU law, resulting in the invalidation of the Safe Harbour.

It is noteworthy that Koen Lenaerts, President of the ECJ, stated after the case “[w]e are not judging the U.S. system here, we are judging the requirements of European Union law in terms of the conditions to transfer data to third countries, whatever they be.”223 The case is a slight to the United States system of data protection but it is presented as an analysis strictly on the requirements of EU law.

---

222 Schrems at [105].
This makes sense politically as well as legally as the ECJ’s jurisdiction under the Treaty on the Functioning of the European Union is limited to EU laws presented by EU Member States so it would be inappropriate to comment on the legality of the FISC.224 However the Advocate General’s opinion does examine the politically sensitive background to the case. This, along with the highly useful work of the Art 29 WP, allows a broader analysis of adequacy to be ventilated and provides useful context to the narrow ratio of Schrems in the ECJ.

The case analysis is broken down into four areas: the powers of the National Supervisory Authorities; the detection and supervisory mechanisms provided by Safe Harbour; whether the limitations and derogations provided by the Safe Harbour were precise, clear and accessible; and Safe Harbour validity in light of the requirements of proportionality and necessity.

A Framework for Analysis: Four European Essential Guarantees

After the invalidation of the Safe Harbour in Schrems the Art 29 WP assessed the jurisprudence of the ECJ relating to art 7, 8 and 47 of the Charter, as well as the jurisprudence of art 8 of the ECHR dealing with surveillance issues. After analysing this jurisprudence, the Art 29 WP issued guidance on what interferences to fundamental rights in a democratic society can be justified.

Adequacy is a level of fundamental rights protection essentially equivalent to that guaranteed in the EU by the Directive read in light of the Charter. The European Essential Guarantees (Guarantees) provide a framework for assessing whether interferences to those fundamental rights are justified, demonstrating the level of fundamental rights protection required and giving body to the meaning of adequacy. Whilst the Guarantees were articulated in light of Schrems, they provide an excellent framework for examining how the meaning of adequacy was shaped in the case.

The Guarantees are:

(1) Processing should be based on clear, precise and accessible rules;
(2) Necessity and proportionality regarding the legitimate objective must be demonstrated;
(3) There must be an independent oversight mechanism; and
(4) Individuals must have effective remedies available.

The first area of analysis in Schrems, examining the powers of the National Supervisory Authorities, can be seen as constituting the third and fourth Guarantees.

The second area of analysis examining the validity of Safe Harbour in the context of effective detection and supervisory mechanisms, concerns the third and fourth Guarantees.

The third area of analysis, examining the validity of Safe Harbour in the context of the clarity, precision and accessibility of the derogations and limitations concerns the first Guarantee.

The fourth area of analysis, examining necessity and proportionality of mass surveillance, concerns the second Guarantee.

The Guarantees are assessed on an overall basis in Court however they will separated for the purpose of clarity in this analysis.225

B The Powers of National Supervisory Authorities

The first issue area of analysis concerned the powers and independence of National Supervisory Authorities generally, and the Irish Data Commissioner specifically, when asked to investigate a complaint about a data transfer presumed adequate by a European Commission decision.

Under art 28 of the Directive, supervisory authorities must be endowed with investigatory powers and operate with complete independence. If the Irish Commissioner was bound by the European Commission Safe Harbour decision and could not investigate the validity of Schrems’ complaint, as the Irish Commissioner contended, the Commissioner would not be independent.

Whilst the Directive does not define complete independence, *Commission v Germany* held it to be acting “completely freely, without taking any instructions or being put under any pressure.” Additionally the decisions of the authorities, as guardians of the right to private life, were required to be above any suspicion of partiality.

*Commission v Hungary* also held independent supervisory authorities to be an “essential component” of protecting individuals’ data and required those agencies to be free from any “external influence in whatever form, whether direct or indirect, which may have an effect on their decisions.” Indeed mere risk of political influence over decisions of the authorities would be enough to compromise independence. It is noteworthy that Ireland has been criticised for insipid enforcement of corporate regulation to encourage foreign direct investment. Whilst this is predominately in tax and company law, the difficulty faced by Schrems in bringing his complaint has extended criticisms of the lack of enforcement to data protection also.

Beyond the case law of the ECJ, the independence of supervisory authorities was found to “derive from the primary law of the European Union” including art 8(3) of the Charter and art 16(2) of the Treaty on the Functioning of the European Union.

Using the language of earlier cases, *Schrems* held independence to be an “essential component” of protecting individuals’ personal data. This also mirrored the language of Advocate General Bot who stated independent supervisory authorities

---

226 *European Commission v Germany*, at [18].
227 At [36].
228 *European Commission v Hungary*, at [48].
229 At [51].
230 At [53].
231 *Schrems* at [40].
are an “essential component”\textsuperscript{232} and “at the heart of the European system” of personal data protection. He stated independent supervisory authorities were a necessary feature for an adequacy finding\textsuperscript{233} and that depriving the supervisory authorities of the ability to investigate the Commission decision would be contrary to the protection of fundamental rights and freedoms, specifically privacy, and would violate the principle of independence.\textsuperscript{234}

Whilst \textit{Schrems} reaffirms the importance of independence in data protection oversight, analysing the powers of the National Supervisory Authorities from a purely legal perspective obscures an important ancillary issue. Adequacy of course has two sides, the content of the rules and their enforcement. Even if the oversight mechanism has sufficient powers and is independent, it must have the resources to fulfil its duties. In 2015 the Irish Data Protection Commissioner received nine hundred and thirty two complaints which were opened for investigation. Although a number of complaints were resolved informally, formal decisions were given in only fifty two cases, a rate of 5.6 per cent and the office had a budget of approximately EUR 3,000,000.\textsuperscript{235} In 2014, nine hundred and sixty complaints were received with formal decisions given in twenty seven cases, a rate of 2.8 per cent, and again the budget was approximately EUR 3,000,000.\textsuperscript{236} Given the prevalence of large multinational data controllers in Ireland, the Irish Data Commissioner specifically, and National Supervisory Authorities generally, appear to be under resourced. From a practical point of view, one can see why the Irish Data Commissioner was hesitant to examine the well-resourced Facebook. It is difficult to believe the ECJ in \textit{Schrems} requiring investigations to be conducted “independently” with “all due diligence” will have much impact if the investigators are not given adequate resources to carry out those investigations.

\textsuperscript{232} Advocate General Bot, above n 220, at [73].
\textsuperscript{233} At [210].
\textsuperscript{234} At [95].
\textsuperscript{235} Helen Dixon “Annual Report of Data Protection Commissioner of Ireland 2015” (Data Protection Commissioner of Ireland, Annual Report, 21 June 2016) at 5.
\textsuperscript{236} Helen Dixon “Annual Report of Data Protection Commissioner of Ireland 2014” (Data Protection Commissioner of Ireland, Annual Report, 23 June 2015) at 5.
Ultimately the ECJ found supervisory authorities must be able to investigate transfers, with all due diligence, to protect fundamental rights.\textsuperscript{237} So the first issue for the Court, whether a National Supervisory Authority is prevented from examining if data transferred to another country is adequately protected, if a European Commission decision states that it is adequately protected, must be answered no. To preserve independence, the Court found supervisory authorities must be able to investigate complaints against data transfers even when the transfer is presumed adequate by a Commission decision.\textsuperscript{238} Of course as Commission decisions are presumed lawful until withdrawn, annulled or declared invalid by the ECJ, meaning the Safe Harbour cannot be declared invalid by a National Supervisory Authority, such as the Irish Data Commissioner. However they must be able to investigate the transfers, and then refer their findings to the ECJ.\textsuperscript{239}

The powers of the National Supervisory Authorities, as well as allowing an investigation into the validity of Safe Harbour, also contributed to the invalidity of the Safe Harbour itself. Article 3 of the Safe Harbour controls the conditions under which a supervisory authority in a Member State may suspend data flows through the Safe Harbour. The cumulative criteria were: a substantial likelihood the Safe Harbour Principles were being violated; a reasonable basis for believing the enforcement mechanisms concerned were not taking adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State had made reasonable efforts to provide the organisation with notice an opportunity to respond.

These provisions restrict the ability of supervisory authorities to exercise their powers, including investigatory powers, by setting thresholds for intervention.\textsuperscript{240} The thresholds of “substantial likelihood,” “reasonable basis” and “imminent risk of grave harm” reduce the ability of the supervisory authorities to act and hence undermine their independence. This is incompatible with art 28 of the Directive.

\textsuperscript{237} Schrems, at [63].
\textsuperscript{238} At [68].
\textsuperscript{239} At [52].
\textsuperscript{240} At [101].
read in light of art 8 of the Charter which requires supervisory authorities to examine, “with complete independence,” claims of fundamental rights infringement concerning personal data.\textsuperscript{241}

The ECJ found the implementing power granted by the EU legislature to the European Commission to adopt adequacy decisions under the Directive did not confer the authority to restrict the powers of National Supervisory Authorities. Given the court found the Commission exceeded its competence in restricting the supervisory authorities’ powers through art 3, the article was found to be invalid, bringing the validity of the entire Safe Harbour into question.\textsuperscript{242}

\textbf{C Safe Harbour Validity: Detection and Supervisory Mechanisms}

The reliability of the Safe Harbour as a self-certifying regime was founded “essentially on the establishment of effective detection and supervision mechanisms” which could identify and punish infringements of fundamental rights.\textsuperscript{243} Adequacy has two sides— the content of the rules and their enforcement. The Safe Harbour was initially found to satisfy adequacy however enforcement issues severely afflicted the scheme and eroded the meaning of strong, adequate protection.

\textit{1 Applicable Law}

The Directive is interpreted within a wider body of EU Law—crucially art 7 and 8 of the Charter and art 8 of the ECHR. However when an issue concerning the application or interpretation of the Safe Harbour regime arose, only United States law was applicable.

Annex IV of the Safe Harbour outlined several paths for claiming damages under United States law, including fraudulent misrepresentation of facts, negligent misrepresentation of facts, intrusion upon seclusion and publication of private

\textsuperscript{241} At [99].
\textsuperscript{242} At [104].
\textsuperscript{243} At [81].
facts. However the Safe Harbour being interpreted under United States law was a significant issue for European data subjects—while the Directive provides protection to data subjects generally, protection under the United States Constitution and United States Privacy Act of 1974 was only available to United States citizens and legal permanent residents. This gave almost no protection for European data subjects.

The FISC, who were to oversee the surveillance by United States federal law enforcement and intelligence agencies also provided limited protection—attracting significant criticism from Advocate General Bot. He found the FISC fell considerably short of providing an effective judicial remedy. First, the Foreign Intelligence Surveillance Act provides no protection to European citizens, only United States citizens, and second, the FISC’s proceedings are ex parte and secret.

The normal path for enforcement of the Safe Harbour was the alternative dispute resolution mechanisms which investigated claims and referred cases to the FTC if required. An alternative path existed with organisations being able to nominate the European Union Data Protection Panel to deal with claims concerning human resources data, however relatively few organisations used this path.

Unfortunately the normal enforcement path of the alternative dispute resolutions mechanisms and the FTC was plagued by serious issues. For example they did not have authority to test the legality of fundamental rights infringements from the United States executive. The United States executive did not have to comply with the Safe Harbour as only self-certifying organisations were bound by its terms.

As a self-certification regime, organisations in Safe Harbour were expected to provide a signed letter to the Department of Commerce with contact details, a statement they are binding themselves to the Safe Harbour, a description of the processing operations and a description of the privacy policy and where it can be

---

244 Safe Harbour, Annex IV.
245 But see Judicial Redress Act of 2015.
246 Advocate General Bot, above n 220, at [208].
247 At [21].
248 Schrems at [89].
found in full. However definition issues weakened many privacy policies with the unclear “aggregate information” and “technical data” sometimes used instead of the standard jurisdictional trigger of “personal data.” Moreover some companies attempted to override the definitions in the Safe Harbour agreement by outlining their own definitions, for example by trying to exclude publically available information from being “personal data.”

2 Federal Trade Commission

A troubling authority issue narrowed the jurisdiction of the FTC. The FTC has competence only in deceptive practices affecting commerce- the data controller must be engaged in commerce. However it was unclear whether this included human resources data and up to 30 per cent of organisations participating in the scheme were doing so to import human resources data. There was also uncertainty over whether the processing of personal data in the context of charitable fundraising and other non-commercial activities would engage in the FTC's jurisdiction as they are not “engaged in commerce.”

Interestingly the regulatory stance of the FTC shifted considerably during the Safe Harbour discussions and the aftermath of its implementation. Prior to implementation self-regulation was held to be “the least intrusive and most efficient means to ensure fair information practices” however this belief shifted ultimately resulting in the FTC formally recommending to Congress they enact omnibus privacy legislation.

Astonishingly it was only in 2009 that the FTC launched their first action against an organisation for violating the Safe Harbour. This is some seven years after the

---

249 Safe Harbour, FAQ 6.
250 Bygrave, above n 39, at 66.
252 Rubinstein, above n 73, at 361.
first European Commission Staff Working paper first identified key weaknesses. The FTC did not protect the data of European data subjects through the Safe Harbour.

3 Alternative dispute resolution mechanisms

A 2008 study by Australian consulting company Galexia documented several of the key weaknesses of the alternative dispute resolution mechanisms under the Safe Harbour. Of the 1597 listed participants in the scheme in 2008, only 1109 were current members, with many of the listed members having failed to renew membership. Many no longer existed and some had duplicate or triplicate entries. Only 348 members successfully listed an acceptable dispute resolution mechanism and only 54 of those extended protection to all types of data.

Many Safe Harbour members failed to list a dispute mechanism at all and more than 200 listed mechanisms that were unacceptably high cost - for example 184 organisations selected the American Arbitration Association as their dispute resolution provider which costs between USD 120 and USD 1200 per hour with a USD 950 administration fee and a minimum charge of four hours. This is clearly incompatible with Safe Harbour Frequently Asked Question 11 which states the dispute resolution provider must be “readily available and affordable.”

TRUSTe was one of the main alternative dispute resolution providers nominated by Safe Harbour organisations. However of the 881 requests they received in 2010, only three complaints were deemed admissible and grounded, leading to an organisation changing their privacy policy. The following year they received 879 complaints however only one organisation was required to make changes to its privacy policy. Clearly data subjects were having substantial difficulty resolving disputes in their favour.

---

255 At 8.
256 At 4.
257 At 14.
258 At 22.
Surprisingly, the European Commission Working Paper report of 2004 found the relatively low level of complaints from data subjects as suggesting organisations were in compliance with the Safe Harbour principles. This is a weak conclusion in light of the poor visibility of privacy principles, low success rates for data subjects and high costs. If people do not know their rights, are confronted by high costs and believe their likelihood of a favourable outcome are low they are unlikely to complain. Audits were tentatively proposed in a 2004 European Commission report as a possible means of checking compliance with the Safe Harbour principles. However the report noted they are highly resource intensive and United States companies would likely resist them on the basis of business confidentiality and sensitive information so they were not implemented.259

4 Conclusions

Safe Harbour and self-certification sits uncomfortably with the European jurisprudence holding “complete independence” of national supervisory authorities as an “essential component” of protecting personal data.260 The supervisory authorities in Europe are required to be “guardians of...fundamental rights and freedoms” by the Court of Justice.261

The difference in protection provided in the United States from Safe Harbour is substantial- a Federal Agency with a limited jurisdiction and almost non-existent enforcement working with expensive reactive dispute resolution providers who want to keep the business of the organisation using them. This strongly contrasts with the EU where independent supervisory authorities have a wide mandate and are not explicitly seeking the business of the organisations they are looking to regulate.

Against these strong critiques of the detection and supervisory mechanisms provided by Safe Harbour, it is difficult to see how the mechanism could have

259 Commission of the European Communities, above n 251, at 6.
260 European Commission v Hungary, at [2].
261 Commission v Germany, at [23].
received an initial positive adequacy finding- one gains an impression of the political and economic incentives the parties had to bring about the Safe Harbour.

It is noteworthy that the Galexia study, after finding little improvement had been made after the negative European Commission Staff Working Paper reviews in 2002 and 2004, concluded significant privacy risk continued to exist for consumers. The report recommended the European Commission, the FTC and the Department of Commerce conduct a comprehensive analysis of every entry on the Safe Harbour list and warn European consumers to check the certification date of any organisation publicly claiming to be a Safe Harbour member. The lack of effective detection and supervisory mechanisms was clearly known prior to Schrems.

Advocate General Bot concluded the ineffectiveness of the detection and supervision mechanisms constituted an interference with the right to an effective remedy under art 47 of the Charter. Given the above analysis it is difficult to reach any other conclusion. The ECJ found effective judicial review to secure compliance with EU law was a requirement of the rule of law itself. Agreeing with Advocate General Bot's position but strengthening the language of condemnation, the ECJ found the lack of legal remedies for European citizens failed to "respect the essence of the fundamental right to effective judicial protection, as enshrined in art 47 of the Charter." Given independent supervisory authorities are a necessary feature for an adequacy finding and are at the heart of the European system of personal data protection, the Safe Harbour clearly falls short of adequacy on this point.

There is a troubling concern that Safe Harbour not only fell short of the requirements of adequacy, but that adequacy withered as a standard of protection with the Safe Harbour. The length of time Safe Harbour was operating and the failings of the detection and supervisory mechanisms reveal considerable weakness in the supposedly adequate protection.

---

262 Connolly, above n 254, at 17.
263 Advocate General Bot, above n 220, at [173].
264 Schrems at [95].
265 Ibid.
266 Advocate General Bot, above n 220, at [210].
C Safe Harbour Validity in Light of the Derogations and Limitations: Clear, Precise and Accessible.

Building on art 52(1) of the Charter, the ECJ in *Michael Schwarz v Stadt Bochum* outlined the requirements for fundamental rights limitations. The limitations must: be provided by law; respect the essence of the fundamental rights; be in accordance with the principle of proportionality; be necessary; and genuinely meet general interest objectives recognised by the EU or meet the need to protect the rights and freedoms of others.\(^\text{267}\) If the Safe Harbour fails this threshold then it will be incompatible with EU law.

Broadly, the analysis of the derogations and limitations concerns two of the Guarantees. First, processing should be based on clear, precise and accessible rules. Second, necessity and proportionality with regard to the legitimate objectives pursued must be demonstrated. The Guarantees are closely linked, for example a proportionate measure must be limited in scope, which requires clear, precise rules, however for ease of understanding the Guarantees will be analysed independently.

Examining the derogations and limitations in the Safe Harbour is crucial to gaining an understanding of the protection provided by adequacy. If the Safe Harbour protections, initially found to be adequate, can be easily circumvented, then adequacy as a high standard of data protection suffers.

For an interference to be in accordance with the law it must have some basis in domestic law and be compatible with the rule of law,\(^\text{268}\) in that is adequately foreseeable, accessible and formulated with sufficient precision.\(^\text{269}\) To meet this requirement the law must protect against arbitrariness and provide, with sufficient clarity, the scope of discretion conferred on competent authorities.\(^\text{270}\)

In contrast to the strict approach to limitations in the Directive which are to be interpreted narrowly and are shaped by the ECHR, the Charter and national...

\(^{267}\) *Case C-291/12 Michael Schwarz v Stadt Bochum* ([CJEU 17 October 2013]) at [34].

\(^{268}\) *MM v United Kingdom* [2012] ECHR 1906 at [193].

\(^{269}\) *Huvig v France* [1990] ECHR 9 at [26].

\(^{270}\) *MM v United Kingdom*, above n 268, at [193].
constitutional laws, the Safe Harbour substantially widened the available exceptions and limitations through Annex I paragraph four.

The fourth paragraph of Annex I allowed the principles of the Safe Harbour to be limited (a) “to the extent necessary to meet national security, public interest or law enforcement requirements” and (b) when case law, statute or government regulation produced conflicting obligations. This gave national security, public interest and law enforcement requirements primacy over the Safe Harbour principles.

Writing an opinion comparing the Safe Harbour and the Directive, Professor Franziska Boehm found it was easily possible to circumvent the protections by transferring the personal data to third parties or the government under United States law. Any legal authorisation, be it federal, state or local, could override the Safe Harbour protections. This greatly expands the possibilities for circumvention and accordingly she felt the Safe Harbour could not be regarded as adequate.

Advocate General Bot felt as “legitimate interests” was not defined in the Safe Harbour it left considerable uncertainty as to the scope of permissible derogations under Annex I paragraph four (b), which he saw as contrary to art 7, 8 and 52(1) of the Charter. He believed the general and imprecise nature of the derogations under (b) as being sufficient in itself to prevent the scheme from ensuring an adequate level of protection. As the Safe Harbour could be disregarded under (b) whenever the scheme conflicts with a United States law, Advocate General Bot felt the scheme was incompatible with the condition that derogations are limited as to what is strictly necessary. It is difficult to disagree with Professor Boehm and

---

271 Commission of the European Communities, above n 181, at 6
272 Schrems, at [84].
273 At [86].
275 At 8.
276 Advocate General Bot, above n 220, at [181].
277 At [183].
278 At [182].
Advocate General Bot given the breadth of legal authorisations allowing an overriding of the Safe Harbour.

Advocate General Bot also found “public interest” and “law enforcement requirements” to be vague under Annex I paragraph four (a). Whilst public interest and law enforcement are legitimate aims they are not defined in the Safe Harbour creating uncertainty over their scope. He found “national security” was the only exception under Annex I paragraph four (a) capable of sufficient precision to be an acceptable limit on fundamental rights.\textsuperscript{279} Crucially however the Safe Harbour did not contain rules on how the interferences would be limited when the United States pursued national security nor how effective legal protection could protect against that interference.\textsuperscript{280} Whilst states receive a fairly wide margin of appreciation when selecting the means to protect national security,\textsuperscript{281} and secret surveillance can be perfectly legitimate, there must be adequate safeguards to prevent surveillance from “undermining or even destroying democracy under the cloak of defending it.”\textsuperscript{282}

The ECJ agreed with Advocate General Bot’s analysis holding the settled case law of the Court regarding interferences with the fundamental rights contained in art 7 and 8 to require “clear and precise rules governing the scope and application of a measure” as well as minimum safeguards.\textsuperscript{283} The lack of clarity over the scope of surveillance and the ineffective safeguards discussed clearly conflict with these requirements- there is no limit to the scope of discretion conferred on authorities in the United States under the Safe Harbour when pursuing national security objectives.\textsuperscript{284} I believe not only is the Safe Harbour short of the requirements for clear, precise, accessible rules governing interferences with fundamental rights, it is considerably short. That any legal authorisation in the United States can override

\textsuperscript{279} At [184].
\textsuperscript{280} Schrems, at [88].
\textsuperscript{281} Weber and Saravia v Germany [2006] ECHR 1173 at [106].
\textsuperscript{282} Szabó and Vissy v Hungary [2016] ECHR 579 at [57].
\textsuperscript{283} Schrems, at [91].
\textsuperscript{284} At [88].
the Safe Harbour protections makes the schemes initial positive adequacy decision incredibly perplexing.

C Safe Harbour Validity in Light of Derogations and Limitations: Necessity and Proportionality

Adequate protection requires a level of fundamental rights protections essentially equivalent to that provided by the Directive. If the limitations in the Safe Harbour do not satisfy necessity and proportionality then adequacy will not be satisfied.

In EU law, limitations are subject to the principle of proportionality and may only be made if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The ECJ held “above all” that to protect the fundamental right to private life the limitations to the protection of personal data must apply only in so far as is “strictly necessary.”²⁸⁵

The Court was uncompromising in finding the Safe Harbour to be well short of requiring limitations to apply only as is strictly necessary. Both the access and subsequent use for mass surveillance purposes constituted an interference which was not strictly necessary.²⁸⁶

Additionally the Court noted the European Commission itself had found the United States authorities could process EU personal data beyond what was “strictly necessary and proportionate to national security” through the Safe Harbour scheme.

Nevertheless proportionality and necessity, which are crucial to understanding whether a limitation on fundamental rights is acceptable, receive only light analysis in both Schrems and the wider case law of the ECJ.

Usefully, the Art 29 WP has released an opinion on the meaning of proportionality and necessity in the context of law enforcement measures which interfere with

²⁸⁵ At [92].
²⁸⁶ At [93].
individuals’ right to privacy and data protection. They outline that as the requirements of necessity and proportionality developed from the case law of the ECtHR under art 8 of the ECHR, the case law of the ECtHR can provide guidance on the meaning of necessity and proportionality. The meaning, scope and application of the concepts of necessity and proportionality under EU law are held to be no less than under art 8 of the ECHR.287

The case law of the ECtHR has provided three criteria which must be satisfied when examining interference with fundamental rights: (i) the interference must be in accordance with the law; (ii) the interference must be in pursuit of a legitimate aim; and (iii) the interference must be necessary in a democratic society. Failure to satisfy all the criteria will result in an interference with fundamental rights being unjustified.

The first two criteria were examined in the previous section however the third, that an interference must be necessary in a democratic society, is multifaceted and requires further analysis.

The Art 29 WP has stressed the importance of necessity not being interpreted too broadly, as this would allow for the circumvention of fundamental rights, nor should it be interpreted too strictly, as this may set too high a bar, restricting perfectly legitimate activities.288

The case law of the ECJ is light on what is meant by necessary however the ECtHR has found “necessary” as being “not synonymous with indispensable...neither has it the flexibility of such expressions as ‘admissible,’ ‘ordinary,’ ‘useful,’ ‘reasonable’ or ‘desirable.’”289

Three tests have developed to determine whether a measure is necessary in a democratic society. They are: (i) whether there is a pressing social need; (ii)

287 Article 29 Working Party “Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector” (536/14/EN WP 211, Adopted 27 February 2014) at 4.
288 At 6.
289 Handyside v United Kingdom [1976] ECHR 5 at [48].
whether the interference caused by the measure is proportionate to the legitimate aim; and (iii) whether the reasons given to justify the interference are relevant and sufficient. The third test is really an amalgamation of the prior two tests in that relevant and sufficient reasons justifying an interference exist only if a pressing social need exists and the measure is proportionate. However research and surveys can be used to support the analysis under the third approach.\(^{290}\)

The Court in *Schrems* found legislation allowing generalised access to personal data is not limited to what is “strictly necessary”\(^{291}\) with generalised access to personal data violating the “essence of the fundamental right to respect for private life” under art 7 of the Charter.\(^{292}\) However the Court did not indulge in a full explanation of how this conclusion was reached. This is disappointing as the necessity and proportionality of mass surveillance sit at the core of the conversation about regulating data in the modern world. In order to understand the Court’s conclusions, I will examine mass surveillance under the necessity and proportionality tests.

I use the first two tests but will use research and surveys to make the analysis more rigorous. The tests share similarities and whilst separated here for clarity, should be seen as two methods of answering the same question- is an interference necessary and proportionate in a democratic society?

1 *Test one: pressing social need*

Reviewing the jurisprudence in the ECtHR, the Art 29 WP highlighted several factors for assessing pressing social needs. They are: whether the issue, if left unaddressed, may result in harm or have some detrimental effect on society or a section of it; whether there is evidence a measure may mitigate such harm; what the broader societal, historic or political views of society on the issue are; and whether opposition views have been sufficiently taken into account.\(^{293}\) “Pressing” is held to imply a level of urgency, immediacy or severity to the need.

\(^{290}\) Article 29 Working Party, above n 287, at 11.

\(^{291}\) *Schrems* at [93].

\(^{292}\) *Schrems* at [94].

\(^{293}\) Article 29 Working Party, above n 287, at 8.
Whether or not an interference corresponds to a “pressing social need” is fluid over time and inherently subjective. For example the ECtHR had to find whether the law criminalising consensual homosexual sex was “necessary” in Northern Ireland. Changing societal views and insufficient evidence of harm meant the law was not remedying a pressing social need and hence was not “necessary.”\textsuperscript{294} Whilst necessary interferences with fundamental rights in the interests of national security has long been at issue, it has received particularly sharp attention in the public dialogue after 9/11.

(a) Whether the measure mitigates against harm

Terrorism is the current harm to be countered when mass surveillance measures infringing on fundamental rights are being justified. However there is little evidence mass surveillance mitigates the harm of terrorism. Indeed Senator Patrick Leahy speaking at a Judiciary Committee in December 2013 stated the oft cited statistic that 54 terrorist plots had been thwarted by mass surveillance was “plainly wrong” and the American people had an “inaccurate impression of the effectiveness of NSA programs.”\textsuperscript{295} This incorrect impression extends to Ireland with Hogan J’s comments in the interlocutory judgment in Schrems that the surveillance programs had “undoubtedly saved many lives.”\textsuperscript{296}

New York Times reporter Charlie Savage made requests for evidence of useful mass surveillance leads under the Freedom of Information Act in the United States, finding little value in the mass surveillance programs. The Federal Bureau of Investigation field officers who had to scrutinise the leads generated from one system found the tips so frequent yet unimportant they reported back “you’re sending us garbage.”\textsuperscript{297}

Looking to the potential benefits of modern scientific techniques, Edward Snowden described the current situation of NSA data collection for terrorist identification as

\textsuperscript{294} Dudgeon v United Kingdom [1981] ECHR 5 at [60].
\textsuperscript{296} Maximillian Schrems, above n 117, at [5].
“analysis paralysis.” He believes excessive information is collected making it impossible to prioritise, narrow and exploit the data. It occurs due to the base rate fallacy- attempting to identify exceptionally rare data points, terrorists, from huge data sets, produces high levels of type one as well as type two errors. Respectively, they are identifying of innocents as suspects and failing to identify real criminals. Epidemiologists know this fallacy and hence try to screen all older women for breast cancer but not all younger woman (who have a lower incidence rate). If all younger women were scanned then the number of type one errors would waste oncology resources on cancer free females, with significant harm resulting from unnecessary surgeries. From a mathematical perspective, mass surveillance of individuals fails to mitigate harm. Instead it provides excessive and low quality predictions with substantial resource and privacy costs.\textsuperscript{298}

As an interesting thought experiment beyond the case, the subtest of whether an issue, if left unaddressed, may have a detrimental effect on society or a section of it, can be applied as a meta-analysis to big data analytics generally. Big data analytics, rather than the problems they are looking to mitigate, may produce detrimental effects. For example, Harvard Professor Latanya Sweeney has found big data bias creeping into algorithms resulting in the racial profiling the black community in the United States.\textsuperscript{299} Additionally data analytics setting the bond amounts and sentence lengths in Florida are still used even though the algorithm commits type one errors against black defendants twice as often as whites (incorrectly labelling a defendant as likely to commit a future crime when they do not).\textsuperscript{300} Even the oft cited success of Google Flu Trends mentioned in the Literature Survey consistently over predicts flu prevalence- reliance on it could cause a significant distortion of hospital resource allocation.\textsuperscript{301} There is a ‘Big Data Hubris’ that pervades big data generally and mass surveillance specifically, where foundational issues of measurement and reliability

\begin{thebibliography}{9}
\bibitem{Sweeney} Latanya Sweeney “Discrimination in Online Ad Delivery” (2013) 56(5) Communications of the ACM 44.
\end{thebibliography}
are substituted for quantity. Further research is needed on the detriment caused by the misguided belief in the accuracy of big data in a mass surveillance context.

(b) What are the broader societal, historical and political views?

Mass surveillance is a difficult, politically charged area where fundamental rights are often perceived as relatively unimportant and threats are overestimated. The pressing social need test may lose effectiveness to the extent it gives genuine weight to inaccurate societal views on mass surveillance to protect national security. Certainly the broader societal, historical and political views can provide useful context to why public support for mass surveillance persist however I find it concerning that inaccurate opinions on the efficacy and necessity of mass surveillance could be given weight by the Court.

Interestingly only 42 per cent of those surveyed from Spain, Germany, Sweden, Netherlands, United Kingdom, France, Greece, Italy, Poland and Hungary believe human rights should be a top foreign policy goal when surveyed by the Pew Research Centre.

In the aftermath of Edward Snowden’s revelations of mass surveillance 47 per cent of people in the United States believed counter terrorism mass surveillance programs had gone too far in restricting fundamental rights with 35 per cent believing the programs had not gone far enough. However in the aftermath of the San Bernadino and Paris shootings in 2015 56 per cent of people in the United States believed the programs had not gone far enough with only 28 per cent believing the programs to have gone too far in restricting fundamental rights. This is a substantial change in belief over a relatively short period. Additionally in the United States 58 per cent of individuals surveyed believed the use of torture on suspected

---

302 At 1203.
terrorists could be justified.\textsuperscript{305} These societal beliefs do not sit comfortably with a high standard of fundamental rights protection.

Despite double digit decreases in recorded violent and property crime in the United States since 2008, only 15 per cent of all voters, and 5 per cent of all Donald Trump voters, believe crimes rates have been reduced.\textsuperscript{306} Moreover in the United States the majority of voters believe the NSA’s mass surveillance programs help prevent terrorist attacks in the United States, with only 28 per cent believing they do not.\textsuperscript{307} Clearly there is significant divergence between the facts and the broader societal and political views.

Given the intensity and emotion surrounding media coverage of terrorism it is perhaps unsurprising the broader societal and political views of terrorism in the United States overestimate its mortality and overestimate the effectiveness of the mass surveillance tools. Weapons of mass destruction sound terrifying, terrorist attacks are graphic and mortifying examples of the harm humans can inflict on each other—many have an understandable desire to give the government sufficient powers to remedy this. However even if the temptation for many is understandable, I do not think it should be given weight given the lack of efficacy of the mass surveillance programs and the very real fundamental rights infringements that mass surveillance entails.

\textbf{(c) Whether opposition views have been sufficiently taken into account}

28 per cent of United States citizens after the San Bernadino believed mass surveillance programs have go too far in violating fundamental rights. It is unclear whether their views have been taken sufficiently into account.

Certainly they are joined by a significant caucus of legal and political academics opposing the current intrusions on fundamental rights made in the interests of

\begin{flushleft}
\textsuperscript{305} Richard Wike “Global opinion varies widely on use of torture against suspected terrorists” (9 February 2016) Pew Research Centre <www.pewresearchcentre.org>.
\end{flushleft}
national security. Even if lawyers, as Schrems discovered when he looked for legal representation, are less willing to support fundamental rights ahead of the business of multinational data controllers.

But opposition views have a difficult time effectively permeating the public discourse. Opposing mass surveillance can be seen not as pro human rights, but as pro-crime. “If you have nothing to hide you have nothing to fear” is a well fed narrative employed by the media and the political machinery to silence opposition views. It plays to the comfortable but cognitively dissonant belief that only miscreants are under constant surveillance. Opposing mass surveillance can be labelled as unpatriotic- it is telling United States legislation concerning mass surveillance have been deceptively labelled the Patriot Act and the Freedom Act.

The phrasing of opposition view is also concerning. It structures the debate as being between national security and privacy. However national security and privacy can be mutually reinforcing, for example increasing data security at government agencies can prevent blackmailing and increase privacy- the true opposing views may be between liberty and control.308

(d) Conclusion on pressing social need test

Ultimately in spite of difficulties with examining the broader societal, historical and political views, as well as considering whether and what oppositions views have been sufficiently taken into account, mass surveillance would fail a pressing social need test- at the very least on the grounds it does not effectively mitigate against terrorism. There is little evidence mass surveillance mitigates against the harm of terrorist attacks and the “urgency” and “severity” of the issue appear in the broader societal views but overinflated in light of the statistics.

2 Test two: proportionality

Proportionality requires interferences to go no further than required to fulfil the legitimate aim pursued. If the Safe Harbour allows disproportionate interferences

---

then it cannot provide adequate protection. The Art 29 WP has found proportionality to require a close analysis of: whether the proposed measure is limited in scope; whether safeguards are in place; the severity of the issue and the harm which society could be exposed to; and the benefits of the proposed measure over existing measure.\textsuperscript{309}

(a) Limited in scope.

Crucially the Court in \textit{Schrems} found the Safe Harbour did not contain any rules limiting interferences with the fundamental rights of European data subjects when United States entities pursued national security.\textsuperscript{310} Compounding this were the lack of references to effective legal protection against such interferences.\textsuperscript{311} Consequently the Safe Harbour did not appropriately limit the scope of fundamental rights interferences.

Retention of DNA and fingerprint samples by Police in the United Kingdom was held to be disproportionate and hence not necessary in a democratic society in \textit{S \& Marper v United Kingdom}.\textsuperscript{312} When considering whether the measure was proportionate and a fair balance between competing private and public interests the Court was struck by the “blanket and indiscriminate nature” of the retaining powers and was concerned there was no differentiation of the seriousness of alleged offences or the age of the suspects.\textsuperscript{313} Indeed individuals could have their fingerprints and DNA samples taken in connection with minor, non-imprisonable offences. This reasoning clearly applies to the surveillance permissible under the Safe Harbour as not only are the powers blanked and indiscriminate, all individuals whose data passes through the scheme can have their fundamental rights infringed, a larger set than just those charged with offences.

\textit{Digital Rights Ireland} in the ECJ examined the issue of whether a data retention directive, pursuing the legitimate objective of national security, satisfied the

\textsuperscript{309} Article 29 Working Party, above n 287, at 10.
\textsuperscript{310} \textit{Schrems}, at [88].
\textsuperscript{311} At [89].
\textsuperscript{312} \textit{S \& Marper}, above n 155, at [125].
\textsuperscript{313} At [35] and [119].
principle of proportionality. The Court found it was not proportionate as: (i) the measure covered all individuals and all means of electronic communications without any differentiation, limitation or exception being made in pursuit of fighting crime; (ii) the measure had no objective criterion limiting access and subsequent use of the data by the authorities to what was strictly necessary and did not have any substantive or procedural conditions regulating the processing of the data; of particular concern was that access was not conditional on prior court review; (iii) there was no objective criteria for determining the specific data retention period; (iv) there were no sufficient safeguards ensuring protection of the data against abuse; and (v) the measure did not require data to be retained within the EU.  

In the Safe Harbour there was no required relationship between the data retained and a threat to public security- even a simple relationship like time period or a geographic zone or something more complex like a nexus of individuals likely to be involved in serious crime. Instead individuals for whom there is no evidence of any remote link at all with serious crime were having their data processed. Given that the mass surveillance underpinning Schrems concerned the content of data rather than metadata as in Digital Rights Ireland, concerns are particularly pronounced.

Additionally whilst in Digital Rights Ireland the Court found national security to be a legitimate aim, the storing of data for up to two years was a disproportionate intrusion into the private lives of customers whose data is retained without any suspicion. The mass surveillance mechanisms using the personal data flowing through Safe Harbour are even more alarming given they do not have a time limit for deletion.

314 Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (CJEU 8 April 2014) at [59]-[69].
315 Ibid.
316 At [64]-[65].
Ultimately the generalised rather than limited access by public authorities, as well as the unlimited data retention period, was held to compromise the essence of the fundamental right to respect for private life guaranteed by art 7 of the Charter.\(^{317}\)

(b) Safeguards

Crucially the Safe Harbour did not contain rules on how the interferences would be limited when the United States pursued national security nor how effective legal protection could protect against that interference.\(^{318}\) As shown by the earlier analysis, the alternative dispute resolution mechanisms and FTC were clearly falling short of acting as sufficient safeguards.

The lack of safeguards in \textit{S & Marper} was decisive as there were no independent reviewing of the justification for retaining suspects’ data and there were limited possibilities for acquitted suspects to have the data removed.\(^{319}\) The need for safeguards was held to be “all the greater” when personal data processing is automatic and used for police purposes- this clearly applies to the automatic processing used for mass surveillance through the Safe Harbour.\(^{320}\) Given the criticism of the safeguards under the effective detection and supervisory mechanisms section, the interference with fundamental rights in \textit{Schrems} could not be considered as sufficiently safeguarded against.

(c) Severity of the issue and harm which society could be exposed to

Examining the magnitude of terrorism harm is a difficult exercise. However looking at the number of fatalities per year in the United States, including perpetrators, gives an interesting perspective. In 2001 there were 2,908 deaths, 2902 from the 9/11 incident alone. In the following thirteen years, six of the years had zero deaths, four years had between one and six deaths, and the two highest years had eighteen and seventeen deaths. This results in a mean number of deaths of four per year over the

\(^{317}\) \textit{Schrems} at [94].
\(^{318}\) At [88].
\(^{319}\) \textit{S & Marper}, above n 155, at [119].
\(^{320}\) At [103].
2002-2014 timeframe. Including 9/11, from 1999-2014 the mean number of United States fatalities in the United States was 186 deaths per year with a total of 2,981 deaths. To contextualise this over 22,000 Americans died from overdosing on prescription opioids in 2015. Additionally over 600,000 people die of heart disease in the United States every year.

Accidents in well understood systems, such as car crashes, produce relatively minimal social disturbance beyond the families and friends of direct victims. However incidents involving unusual means of harm, such as nuclear attacks or anthrax scares, are poorly understood and are interpreted by many as omens of further disasters causing disproportionate psychological and political impacts. Even though the harms of terrorism may be relatively small compared to car crash mortality, the perception of the terrorism harm is substantial and hence legislators are under significant pressure to appear to tackle the issue.

Whilst any death is significant, contextualising the lives lost to terrorism against other causes of mortality gives an indication of the urgency and severity of the need to combat terrorism through mechanisms that seriously infringe fundamental rights. It is noteworthy in a survey conducted just before the 2016 United States Election, nearly three quarters of Trump supporters and two fifths of Clinton supporters saw terrorism as a “very big problem.” Whilst fear of terrorism is undoubtedly prevalent, the harm when measured by mortality is relatively small.

Once again moving from the harm mass surveillance is looking to mitigate to looking at the harm actually caused by mass surveillance is a useful exercise. There are some significant economic harms flowing mass surveillance. For example economic losses

323 Centre for Disease Control "Heart Disease Facts" (August 2015) United States Department of Health and Human Services <www.cdc.gov>.
to United States based cloud computing firms is estimated to be between USD 22,000,000,000 and USD 180,000,000,000.\[^{326}\]

It is also noteworthy the Court in *S & Marper* was willing to consider harms from future use of personal data, with undiscovered technology, as legitimate and relevant to examining an interference with fundamental rights.\[^{327}\] This was in the context of DNA material being put to future uses. Big Data analytics is likely to allow more sensitive intuitions about individuals in the future than it does today. Given the lack of data minimisation and ability to store personal data over the long term, the processing of personal data by the NSA arguably needs to be contextualised not only by the fundamental rights infringements occurring today, but those that might occur with further processing to stored personal data as technology develops.

(d) Benefits over proposed measures

The requirement that a measure has benefits over existing measures again sits uncomfortably in the context of mass surveillance. One analysis of terrorist attacks within the United States since 9/11 found metadata collection had “no discernible impact on preventing acts of terrorism.”\[^{328}\] Additionally the think tank New America, reporting on the NSA, found traditional investigative methods, being tip offs, informants and targeted surveillance, provided the impetus for most case investigations. The contribution of NSA’s mass surveillance programs was labelled as “minimal.”\[^{329}\]

It is hard to see the measures as proportionate in light of the disputed benefits over traditional policing methods which interfere less with fundamental rights. In *Schwarz* whether a data processing measure was “necessary” required an examination of other measures which will interfere less with the fundamental rights under art 7 and 8 of the Charter but would still contribute to objective of the

\[^{327}\] *S & Marper*, above n 155, at [71].
legislation. Tip offs, informants and targeted surveillance with a warrant in this context all provide genuine benefits with substantially less privacy and data protection infringements.

(e) Conclusion on Proportionality test.

Given the broad scope, lack of safeguards, contentious magnitude of the harm being addressed and lack of benefits of over other measures, mass surveillance appears to be a significantly disproportionate interference with fundamental rights.

3 Conclusion on Safe Harbour validity in light of necessity and proportionality

Advocate General Bot found the mass, indiscriminate surveillance being undertaken in the PRISM program was “inherently disproportionate” and consequently was an unwarranted interference with the fundamental rights provided under art 7 and 8 of the Charter. Mass surveillance was held to be an “extremely serious” interference due to its secrecy, the large volume of personal data involved and the substantial number of data subjects affected. Indeed Advocate General Bot found any third country with rules of law permitting mass and indiscriminate surveillance could not be considered to offer adequate protection under any circumstances.

However the ECJ took a slightly unusual step in that art 1 of the Safe Harbour was not declared invalid because it allowed for disproportionate and unnecessary interferences with fundamental rights, providing a level of protection of fundamental rights lower than that required by adequacy. Instead, although art 1 stated the Safe Harbour provided adequate protection, the ECJ found the Safe Harbour contained insufficient findings regarding the international commitments and domestic laws by which the United States actually ensured an essentially equivalent standard of protection. Given the requirement to state the United States ensures adequate protection with duly stated reasons, the ECJ declared the

330 Schwarz, above n 267, at [46].
331 Advocate General Bot, above n 220, at [171],[200] and [201].
332 Schrems at [83].
Safe Harbour invalid “without there being any need to examine the content of the Safe Harbour principles.”\footnote{At [98].}

This is an unusually technical point upon which to find the Safe Harbour invalid. It is politically cautious in that it does not aggressively attack the United States data protection system, however it presents as a gloved fist withdrawn at the last moment. The judgment clearly holds the Safe Harbour principles and enforcement to be well below the adequacy standard of essentially equivalent however the invalidation is made on a narrow technical point that insufficient reasons were given by the European Commission when making the positive finding of adequacy. The Court withdrew from a full, explicit statement that the underlying protection of the Safe Harbour was inadequate.

The purpose of invaliding the implementing decision on a technical point would appear to be for future negotiating reasons. If the Safe Harbour was invalidated on account of its principles and enforcement regime, it would be difficult to implement a new, similar scheme. However if the Safe Harbour was invalidated because its implementing decision was not specific and comprehensive enough, this provides more flexibility for establishing a slightly improved scheme.

Ultimately the case fails to rigorously outline the requirements of achieving adequate protection- instead it retreats to the ratio that adequacy implementing decisions must state sufficient reasons for why a country in fact ensures adequate protection.

\textit{E Key Points}

The central finding of Schrems is that adequacy requires a level of protection of fundamental rights that is essentially equivalent to that guaranteed within the EU.

From a legal perspective, independent and effective detection and supervisory mechanisms are required and individuals must have legal remedies available.
Crucially any processing that interferes with fundamental rights must be based on clear, precise and accessible rules. Additionally necessity and proportionality regarding the national security interest pursued must be demonstrated.

*Schrems* disappointingly failed to complete a thorough analysis of the necessity and proportionality of mass surveillance.

However under my own analysis I suggest mass surveillance falls considerably short of satisfying the requirements of necessity and proportionality.

The case must be understood in its political context. Clearly the EU and the ECJ were hesitant to sour diplomatic relations with the United States.

The Safe Harbour evidently provided inadequate protection of data from its inception however under significant economic and political pressure it still received a positive adequacy finding.

Disappointingly the final judgment of *Schrems* did not explicitly find the protection provided by the United States data protection regime or the Safe Harbour inadequate. Instead the ECJ found the implementing decision was not thorough enough. This move lacks judicial courage and paves the way for a similar mechanism (the Privacy Shield) to replace the Safe Harbour.

Ultimately the ECJ in *Schrems* failed to seize the opportunity to provide a detailed account of the requirements of adequacy and cannot be seen as a strong upholding of fundamental rights in the EU.
Art 25(6) of the Directive provides an adequacy decision may be given if a country ensures an adequate level of protection, by reason of its domestic law or international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals (emphasis added).

To better understand adequacy then it is useful to examine the rights to data protection and privacy which underpin it. If they are uncertain in scope or the ECJ is inconsistent in asserting the rights under the Charter then adequacy will suffer, especially in light of the strength of the economic and national security interests which can act against those rights.

Curiously when the Charter was first introduced in 2000 the President of the European Commission Romano Prodi outlined the purpose as being “to make more visible and explicit to European Union Citizens the fundamental rights they already enjoy at European level.” However the Charter, rather than just consolidating and making more visible the rights contained in the ECHR, introduced new rights such as the right to environmental protection under art 37 and of course the right to the protection of personal data under art 8. If the right to data protection is simply a restatement of the right to privacy then its inclusion in the Charter may be redundant. On the other hand it may provide additional protection for adequacy if it is distinct from art 7.

Given the Charter’s relative youth the ECJ has benefitted greatly from the experience and expertise of the ECtHR. The relationship between the two Courts has been described as a mutually respectful, informal arrangement, a sort of “common supranational diplomacy.” The right to private life under the ECHR in particular has been useful with the ECJ finding art 7 of the Charter to be given “the same

---

335 At 679.
meaning and the same scope as article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights.” 336

Whilst the corpus of human rights law from the ECtHR gives the right to data protection and privacy under the Charter some stability, the ECJ has been hesitant in firmly asserting art 7 and 8 of the Charter. Indeed whilst the Charter was introduced in 2000 it was not until 2009 that it achieved binding legal status. 337 The ECJ did not cite the Charter for the first six years of the Charter’s existence, preferring to use national fundamental rights protections and the ECHR, although the Court of First Instance did cite the Charter directly during this period. 338

Confusion has occurred as the ECJ has drawn on both the ECHR and Charter to develop its own fundamental rights jurisprudence. For example in Michael Schwarz v Stadt Bochum, a case concerning biometric data on passports, the ECJ examined the requirement that limitations of rights must be “provided by law.” 339 This provision is supposed to import the significant case law of the ECHR which requires an interference to have a basis in domestic law as well as be compatible with the rule of law, in that it is adequately accessible, foreseeable, free from arbitrariness and has sufficient clarity. However the ECJ only analysed whether the interference had a basis in domestic law. 340 Consequently the Court held the law’s validity to be tautologically satisfied by virtue of it being a law, rather than satisfying the requirements of being compatible with the rule of law. These confusions characterise a jurisprudence lacking coherence and hinder the Charter’s development as an independent source of fundamental rights.

The relationship between art 7 and art 8 of the Charter is also beset with unclarity. For example in Volker und Markus Schecke and Eifert art 7 and 8 were found to be

336 Case C-400/10 J McB v L E [2010] ECR I-8965 at [53].
339 At [34].
340 Gloria Fuster “Fighting for your right to what exactly? The convoluted case law of the EU Court of Justice on privacy and/or personal data protection” (2014) Birkbeck Law Review 2(2) 263 at 270.
closely connected with the Court finding the “right to respect for private life with regard to the processing of personal data” was “recognised by articles 7 and 8 of the Charter” implying the two articles combine to form a composite right.\footnote{Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert v Land Hessen [2010] ECR I-11063 at [52].} However treating the rights as one questions whether they can be relied upon independently and art 8 of the Charter implicitly loses its authority to stand alone as a sui generis right if it is always pleaded in conjunction with the right to privacy.

*Digital Rights Ireland*, in which the ECJ declared a Data Retention Directive invalid, also highlights the imprecision of the ECJ’s approach. Initially the Court examined the Data Retention Directive’s impact on the right to private life under art 7 of the Charter, before finding “such a retention of data also falls under article 8 of the Charter”- treating the two rights as providing distinct rather than overlapping protection.\footnote{At [29].} However the separation of the two rights then collapsed with the Court finding the protection of personal data under art 8 to be “especially important for the right to respect for private life enshrined in article 7 of the Charter.”\footnote{At [53].} This locates the importance of art 8 not in the fact it is a fundamental right, but in its relationship to art 7. Curiously, when the Court completed an assessment of the legitimacy of the interferences, the rights were considered together. So what started as a separate analysis of two rights merged to produce one “right to the respect for private life” of which the protection of personal data appeared to be a component.\footnote{Fuster, above n 340 at 274.} Whilst joining the two rights might appear to reinforce the protection they provide, uncertainty results from the ECJ adopting such an inconsistent approach.

The Advocate General Cruz Villalon’s opinion in *Digital Rights Ireland* provides little assistance. He held that legislation justifiably limiting the right to personal data protection under art 8 of the Charter could nevertheless constitute a disproportionate interference with art 7.\footnote{Advocate General Cruz Villalon “Opinion of Advocate General Cruz Villalon on Case C-269/12 Digital Rights Ireland v Minister for Communication, Marine and Natural Resources and Others and Kärntner Landesregierung and Others” (Opinion, ECLI:EU:C:2013:845, Delivered 12 December 2013) at [61].} This suggests the right to privacy provides protection above and beyond the right to data protection. However he then
argues the rights “are so closely linked that they may be regarded as establishing a single ‘right to respect for private life with regard to the processing of personal data.’” It is confusing that two rights should be considered together but an interference could infringe one but not the other.

Schrems failed to rectify any of the uncertainty in the relationship between the right to privacy and the right to data protection. The Court found adequacy under art 25(6) “implements the express obligation laid down in article 8(1) of the Charter to protect personal data” (emphasis added). However it is unclear why there is a focus on art 8 rather than art 7. Particularly given that the Court later found legislation allowing public authorities generalised access to electronic communications compromised the “essence of the fundamental right to respect for private life, as guaranteed by article 7 of the Charter” (emphasis added).

Additionally when considering whether an adequacy decision might have to be reconsidered in light of mass surveillance the Court stressed the “important role played by the protection of personal data in light of the fundamental right to respect for private life.” Again this appears to make the right to data protection subordinate to the right to privacy- with the value of the former flowing from its contribution to the latter.

Whilst drafting art 8 as a right separate from privacy appeared innovative when the Charter was introduced, the jurisprudence of the ECJ has failed to give art 8 an independent existence. It is unclear what, if any, protection art 8 gives outside of art 7. However the youth and uncertain scope of art 7 and 8 of the Charter is not per se a weakness as it can allow for flexibility in the ECJ’s response to blossoming issues for adequacy. In turn that flexibility can be constrained as required by the persuasive but not binding precedent of art 8 of the ECHR.

---

346 At [62].
347 Schrems at [72].
348 At [94].
349 At [78].
However the relationship between art 7 and 8 of the Charter cannot be clearly elucidated from the wider case law of the ECJ and Schrems fails to contribute any clarity to the situation. Ultimately the foundation of fundamental rights on which adequacy is built is unclear- there are relatively few ECJ judgments asserting the fundamental rights to privacy and data protection against strong economic and national security interests. This uncertainty and lack of precedent may have contributed to the ECJ’s decision in Schrems to find the Safe Harbour invalid on technical grounds rather than carrying out a full fundamental rights analysis.

A Further Case Study: Positive Adequacy Decision for Passenger Name Record (PNR) Data.

After the 9/11 terrorist attacks the United States Bureau of Customs and Border Protection wanted PNR data prior to any flights arriving in the United States, for national security purposes.

This left airlines in the EU in a precarious position of potentially violating EU data protection law by complying and violating United States law by refusing. As with the Safe Harbour, a legal and political compromise was pursued balancing the EU’s right to personal data protection and the United States ability to legislate for national security purposes. The European Commission initially informed the United States that PNR data collection would conflict with EU law. However the United States refused to waive the right to penalise airlines refusing to cooperate and subsequently many large airlines granted access to the personal data as requested.\(^{350}\)

The European Commission, in a political knot, adopted a positive adequacy decision for a 2004 PNR agreement with the United States which attracted significant criticism. The European Parliament subsequently challenged the adequacy decision primarily on human rights grounds but also on the basis of the European Commission’s competence to enter such an agreement under the first rather than third pillar of the EU. The ECJ found for the European Parliament in 2006 however

\(^{350}\) Joined Cases C-317/04 and C-318/07 European parliament v Council of the European Union and Commission of the European Communities (CJEU 30 May 2006) at [33].
the decision was decided on competence issues rather than fundamental rights issues, with no privacy concerns examined in the Court.\textsuperscript{351} This politically polite move mirrors the ECJ in \textit{Schrems} invalidating the Safe Harbour on competence and narrow technical grounds rather than on fundamental rights grounds.

The decision by the ECJ invalidating the PNR agreement made no reference to the ECHR or the Charter. This meant new PNR decisions could be achieved so long as a different implementing procedure was adopted.\textsuperscript{352} If the original decision by the ECJ had taken a fundamental rights approach, rather than a competence approach, the subsequent PNR agreements would likely have needed improved fundamental rights protections. Additionally it would have been an excellent opportunity to shape the relationship between the rights to data protection and privacy against national security.

Locating the reasoning in competence issues halted the first PNR decision but has done little to halt subsequent PNR decisions and failed to shape the rights of privacy and data protection. Currently the EU has agreements with Canada, Australia, a new one with the United States and negotiations have opened with Mexico. The most recent PNR agreement was adopted in 2016 and captures significant personal data of individuals entering and leaving the EU.\textsuperscript{353}

The data demanded include up to thirty five different types of information including meal preferences which can indicate religious affiliation. To highlight concerns Paul Ohm uses the concept of “information entropy,” which measures how close a given fact is to being connected to an individual. It is a measure of the uncertainty of the inference chain required to make that connection.\textsuperscript{354} He argues that apparently benign reidentification steps which cause no obvious harm still need to be protected against as they shorten the inference chains required. Crucially the PNR data can contain mobile phone and credit card information which are crucial linking fields.

\textsuperscript{351} At [67].
\textsuperscript{352} Douglas-Scott, above n 338, at 284.
\textsuperscript{354} Ohm, above n 102, at 1749.
These two fields can substantially reduce information entropy and link with other data sets held by other agencies. Arguably then an analysis of whether the collection of PNR data is proportionate needs to be seen against the risks of data sharing between agencies using phone or credit card information as linking fields.\(^{355}\)

The value of PNR data collection is challenged on the basis almost no evidence exists of such data being used to effectively deter or prevent terrorist activity.\(^{356}\) Professor Fred Cate slices the issue poignantly in an American context— if the data mining of PNR data achieves a positive terrorist identification rate of 1 per cent, which is significantly higher than that achieved in publically disclosed records, around 7,500,000 passengers in the United States will be incorrectly identified as potential terrorists each year.\(^ {357}\) This huge processing of personal data has tangible harms beyond privacy invasions, with incorrect placement on no fly lists an obvious illustration.

Rahinah Ibrahim, a Doctor of Philosophy student from Stanford, was denied entry to the United States due to a bureaucratic error.\(^ {358}\) After several years she achieved a pyrrhic victory in that her inclusion on the list was found to be incorrect but she still cannot get a visa to visit the United States. A general review by the Department of Justice Inspector General found that tens of thousands of people are incorrectly placed on the No Fly List with some 35 per cent of the nominations to the list being outdated.\(^ {359}\) In light of the privacy costs and inaccuracies, and that many of the decisions made from the PNR are autonomous with little option for objection, the Art 29 WP has been outspoken in their scepticism of whether PNR systems are proportionate to the alleged security benefit.\(^ {360}\)

\(^{355}\)Douwe Korff and Marie Georges “Passenger Name Records, data mining and data protection: the need for strong safeguards” (Report for Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, 15 June 2015) at 8.


\(^{357}\) At 475.

\(^{358}\) *Ibrahim v Department of Homeland Security* C06-00545 WHA (ND Cal 2014).

\(^{359}\) Korff and Georges, above n 355, at 20.

\(^{360}\) Article 29 Working Party “Opinion 7/2010 on European Commission’s Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries” (622/10/EN WP 178, Adopted 12 November 2010) at 3.
Disappointingly the EU has pushed forward with an internal PNR Directive which would be implemented by 2018. This would establish databases tracking the movements of all individuals travelling into or out of the EU, although Member States can choose to include intra-EU travel as well. A European Data Protection Supervisor had described the proposal as failing to achieve the correct balance between fighting crime and the “rights of the innocent majority to go about their daily lives without undue interference.”

Ultimately PNR agreements in the EU show the reluctance to protect fundamental rights in light of the national security interests of trading partners. The PNR and Safe Harbour experiences show the European Commission is prepared to lower fundamental rights protections for European citizens in order to achieve political compromise with the United States- ultimately lowering the value of adequacy.

The ECJ has shown a willingness to find against the European Commission, which is encouraging, however the reasoning adopted has only provided short term success. The narrow finding of ultra vires in the PNR decision and hence that “the decision on adequacy must consequently be annulled and it is not necessary to consider the [fundamental rights] limbs of the first plea” is disappointing. The fundamental rights pleas were incredibly important. A sharp fundamental rights analysis could have provided some clarity over the meaning of art 7 and 8 of the Charter and would have given support to the Art 29 WP’s criticisms of PNR data collection. Additionally the PNR decision gave the ECJ an opportunity to reinforce the precedent that generalised collection of personal data of law abiding citizens is antithetical to fundamental rights. I believe the ECJ must be more courageous in asserting the Charter against a growing international willingness to interfere with fundamental rights in the pursuit of national security.

**B Fundamental Rights in the European Union Generally**

Plainly there are issues with the scope and shape of the fundamental rights to data protection and privacy under the Charter. However fundamental rights in the EU are

---

also unclear when analysed from a higher level of abstraction. If the fundamental rights of the EU are unsettled or have their authority challenged, then the effectiveness and success of adequacy may suffer. The stability of adequacy demands a stable conception of the fundamental rights it is to protect. I address two primary issues in this section: (i) how an economic focus might reduce the protection provided by fundamental rights; and (ii) how primacy issues might change the protection provided by fundamental rights.

1 Economic issues

The object of the Directive requires the protecting of fundamental rights and freedoms however Member States must not “restrict or prohibit the free flow of data.” A tension exists here between economic pursuits and the rights to privacy and data protection. As Schrems noted, the National Supervisory Authorities must ensure a “fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data.” This is further highlighted in recital 2 of the Directive where data processing systems are required to respect “fundamental rights and freedoms” but also “contribute to economic and social progress.”

Speaking to the Wall Street Journal on the case of Schrems, Koen Lenaerts, President of the ECJ, stated “Europe must not be ashamed of its basic principles: The rule of law is not up for sale. It is a matter of upholding the requirements in the European Union, of the rule of law, of fundamental rights.” When asked whether the judgment sufficiently considered the economic fallout to business he artfully replied “if this is also affecting some dealings internationally, why would Europe not be proud to contribute its requiring of standards of respect for fundamental rights to the world in general.” These comments locate fundamental rights at the core of the EU’s purpose. However the EU’s history and focus on the common market suggest its

362 Art 1(1)-(2).
363 At [42].
364 Pop, above n 223.
centre of gravity lies in the economy rather than human rights as Lenaerts implies.\footnote{Douglas-Scott ”The European Union and Human Rights after the Treaty of Lisbon” (2011) 11(4) HRLR 645 at 645.}

Privacy protection might be lowered if there is an economic focus in the ECJ and there is concern the Charter encourages this by including economic rights as “fundamental rights.” Without a hierarchy of rights well-resourced economic interests could dominate social and political rights in certain contexts. Indeed Professor Ulrich Haltern has described the EU as a “shallow” and “superficial” organisation which “privileges the commercial above all else.”\footnote{Douglas Scott, above n 338, at 1.} Whilst an extreme position, his concerns have basis. For example in \textit{Schmidberger}, freedom of expression, a core human right, was held to be an “equal interest” with the right to the free movement of goods.\footnote{Case C-112/00 Schmidberger v Austria [2003] ECR I-5659 at 81.} Additionally in the cases of \textit{Laval} and \textit{Viking} market freedoms, specifically the right to provide services, outweighed the fundamental right to strike which the court felt had been exercised disproportionately.\footnote{Case C-438/05 International Transport Workers’ Federation, Finnish Seamen’s Union v Viking Line ABP, OÜ Viking Line Eesti, [2007] ECR I-10779 and Case C-341/05 Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet and others [2007] ECR-I-11767.}

The meaning and scope of fundamental rights can drift over time- shaped by those with the resources to litigate. Whilst traditionally conceived of as tools for the powerless against the powerful, rights can come to be used by the powerful against the vulnerable. The concerns are particularly pronounced in the United States experience- corporations have had their political donations protected as free speech\footnote{National Bank of Boston v Belotti 435 US 765 (1978) and Citizens United v Federal Election Commission 558 US 310 (2010).} and have been able to restrict inspections from Occupational Safety and Health workers due to the right against unreasonable search and seizure.\footnote{Marshall v Barlow’s Inc 436 US 307 (1978).} It is a curious point that a corporation may enjoy freedom from unreasonable search and seizure but a United States prisoner may not.\footnote{Proudfoot v Williams 803 F Supp 1048, 1051 (ED Pa 1991).} Fundamental rights can drift over time to protect those with the power and influence to lobby and litigate.
As the Directive requires a balancing of economic progress with the right to privacy and data protection, in the long term the balance may tilt in favour of economic progress— with adequacy withering if the rights to privacy and data protection are not strengthened. Well-resourced lobbying interests in Europe could be expected to align behind “economic” interests. This concern is marked when the history and initial economic focus of the EU’s origins are considered. Adequacy has the difficult task of accommodating the tension between fundamental rights and economic interests. This tension is likely to increase with the emergence and integration of technologies with huge economic benefits but significant privacy concerns— particularly Big Data and artificial intelligence.

2 Primacy issues

Some commentators believe the EU has used fundamental rights as a vehicle for establishing primacy. Under this interpretation fundamental rights are a palatable means to EU supremacy and autonomy rather than an ends themselves, an epiphenomenon of the European project of market integration. However just because the motivations for fundamental rights may be instrumental in nature, the protection provided by those rights is not necessarily weakened— indeed Member States rejecting EU law supremacy in favour of their own rights guarantees could raise protection in some contexts. However to the extent fundamental rights are contested by Member States and international organisations, instability may increase and the credibility of the EU as a fundamental rights organisation may decrease.

Initially the EU eschewed the responsibility of guaranteeing fundamental rights— the European Economic Community, as the EU was formally known, had competence only in economic matters and did not express explicit ambitions to provide fundamental rights protections. National courts and the ECtHR, a Council of Europe organisation, were already guarantors of fundamental rights. However as the EU extended its competence to visas, asylum and criminal matters, fundamental rights became much more relevant to the organisation.372 The rights were initially asserted

---

372 Douglas-Scott, above n 365, at 648.
in case law as general principles of law before being codified in Article 6 of the Treaty on European Union (TEU) and the Charter. This move produced tension in two domains, between the Member States and the EU and between the EU and other international organisations such as the United Nations.

Starting in the 1960s some Member States questioned whether the fundamental rights protections in their constitutions were protected in the realm of European Community law. These concerns arose as whilst the exercise of public power at the national level was subject to constitutional guarantees, supranational action at the European level had no legally binding fundamental rights standards. In response to these concerns, and to prevent Member States answering the question themselves- possibly by declaring the supremacy of their own constitutions- the European Court “discovered” that fundamental rights were a general principle of European Community law drawn from the constitutional traditions common to Member States. These general principles were referenced first in Stauder before being expanded in Internationale Handelsgesellschaft where it was held “respect for fundamental rights forms an integral part of the general principles of [European Community] law.” Guidance on fundamental rights from international conventions, later indicated to include the ECHR and the European Social Charter, was held acceptable in Nold. Against this backdrop there is a difficulty of coherence. The Member States have different constitutional histories- determining which traditions are suitably common is a subjective and trying exercise.

Initially fundamental rights were only used to challenge Community acts rather than Member State acts however this stance shifted over time. In Roland Rutili v Ministre de l’intérieur fundamental rights were alluded to as relevant

---

373 At 648.
376 Ibid.
378 See generally Coppel and O’Neil, above n 375, at 230-240.
considerations for analysing Member State action. Then in *Wachauf v Federal Republic of Germany*\(^{380}\) the Court applied fundamental rights principles directly to Member State acts implementing Community legislation.\(^{381}\) Building on this in *Elleniki Radiophonia Tileorasi v Dimotiki Etairia Pliroforissis* the Court extended their jurisdiction again, implying they could examine all Member State actions against fundamental rights as long as the matters concerned fell within the area of Community Law.\(^{382}\) This is a subtle transfer of power from Member States to the EU.

Member States have been cautious in locating the protection of fundamental rights in EU law rather than their own constitutional law. For example the Federal Constitutional Court in the late 1980s and early 1990s only accepted the supremacy of EU law if EU law guaranteed the fundamental rights protection provided under the German Basic Law.\(^ {383}\) The Czech Constitutional Court, possibly stimulated by the German position, also adopted a conditional acceptance position, finding the Treaty of Lisbon as compatible with Czech constitution rather than accepting it without condition.\(^ {384}\)

The experiences of the European Arrest Warrant (EAW) scheme also disrupt the harmonious view that Member States and the EU have a coherent, stable understanding of how fundamental rights should be protected. As part of an EU security initiative the EAW scheme provides for the arrest and surrender of individuals from one Member State to another for criminal proceedings. The merits of the request and the protection of fundamental rights are taken on trust and the alleged crime does not have to be a crime in both the requesting and surrendering state. Constitutional Courts in Germany, Poland and Cyprus struck down the national laws implementing the scheme on the basis the scheme did not adequately protect fundamental rights.\(^ {385}\)

---


\(^{381}\) Coppel and O’Neil, above n 375, at 238.


\(^{384}\) Douglas-Scott, above n 365, at 681.

\(^{385}\) Douglas-Scott, above n 338, at 278.
Crucially Belgium made a preliminary request from its Supreme Court to the ECJ on the issue of whether the EU’s EAW framework decision was itself null and void, rather than just striking down the implementing laws as occurred in Germany, Poland and Cyprus. The ECJ upheld the EAW framework however the decision has been criticised for only superficially addressing fundamental rights issues and assuring a high level of trust did exist between Member States. Bubbling beneath the assurance were divergent approaches to fundamental rights protections for accused- especially given issues such as abortion, inciting racial hatred and euthanasia are treated very different across Member States.

The EAW experience shows (i) how the EU can press security issues ahead of fundamental rights; and (ii) the instability of fundamental rights between Member States and between the EU and Member States. As Professor Douglas-Scott reminds us, the constitutional traditions of Member States can be a “divisive and fragmenting source, rather than a unifying source, for rights.”

Professor Joseph Weiler believes that whilst the surface language of Stauder and its progeny concern human rights, the “deep structure is all about supremacy.” The ECJ case of Kadi, often heralded as a success for fundamental rights, provides an interesting lens to analyse this quest for supremacy. Mr Kadi, a wealthy businessman, had his assets frozen under a UN resolution on the grounds he was associated with the Al-Qaeda network. Whilst the Court of First Instance found the primacy of the UN did not allow a review of the decision against EU fundamental rights, and that review would cause significant disruption to the international order, the ECJ on appeal found his right to be heard, his right to an effective remedy and a procedural aspect of his right to property had been violated.

The outcome of the case appears to be a victory for fundamental rights against overreaching counter terrorism regulation. Indeed writing on the case one academic

---

386 At 277-282.
387 Douglas-Scott, above n 365, at 670.
388 Coppel and O’Neil, above n 375, at 229.
390 Douglas-Scott, above n 338, at 286.
declared “in the European Union’s flawed system of governance, democracy finds solace in judicial review.”\(^\text{391}\) Whilst justice may have been found in the case, the judgment was particularly concerned with autonomy and primacy. The court stated the “Community must respect international law”\(^\text{392}\) however it went on to hold the European Community was “based on the rule of law, of a constitutional guarantee stemming from the EC Treaty as an autonomous legal system” and that this legal system “was not to be prejudiced by an international agreement.”\(^\text{393}\) There was a clear intention to align EU law with constitutional and national law rather than international law.

The Court could have reached the same outcome for Mr Kadi without focusing on the autonomy of the EU, instead focusing on the EC’s implementation of the UN Security Council order. Choosing not to take that judicial path appears to be a deliberate and direct confrontation between the EU and UN.\(^\text{394}\) Additionally the decision of the ECJ to focus on competence rather than fundamental rights in the PNR agreements provides interesting context to Kadi. If Kadi is an example of fundamental rights overcoming unjust blacklisting then it sits uncomfortably with the European Commission pursuing its own PNR agreements, which have widely known deficiencies. If however Kadi and the PNR agreements are about the assertion of the primacy and autonomy of the EU, then they read together more comfortably.

Analysing how and why the EU has manoeuvred to its current legal relationship with its Member States and the international community may appear to be solely an academic exercise- such a conclusion would be unwise in the context of Brexit. Britain has taken the first step to remove itself from the EU. Supremacy of EU law against British law was a key issue receiving public ventilation in the lead up to the referendum, although issues of cost saving and National Health Service spending appear to have dominated concerns for voters. It is difficult to know the reasoning

\(^{391}\) Takis Tridimas “Terrorism and the ECJ: Empowerment and Democracy in the EC legal Order” (2009) 34 EL Rev 103 at 103.
\(^{392}\) Kadi, above n 390, at [6].
\(^{393}\) At [316].
behind those who voted to leave however the website of the Vote Leave campaign provides interesting context. Under the Why Vote Leave page the campaigners, writing from a British perspective, claim the ECJ “overrules us on everything from how much tax we pay, to who we can let in and out of the country, and on what terms.” The site also puts forward the question “What is this campaign really about?” before starting the answer with “[o]ur political system is stuck. Whichever party is in charge, the Government cannot sort out our problems or deliver their promises because they have to follow EU rules.”

These tensions for supremacy could have consequences for data protection in Europe. First it is worth noting Britain might have a difficult time achieving a positive adequacy decision as a third country. This is particularly in light of the recent Investigatory Powers Act 2016 which expands surveillance powers and requires telecommunications companies to store web history for up to a year—possibly beyond what is strictly necessary and proportionate in the interests of national security. Second, if further countries leave the EU the number of European individuals receiving EU fundamental rights protection will be reduced. And thirdly, as countries leave the EU, the authority of the EU declines. Looking at a hypothetical long term an EU with fewer members will have less impact on data protection law norms internationally. It is noteworthy that some politicians in Europe are already campaigning for further EU exits. For example Norbert Hofer, a far right candidate in Austria has advocated for an Austrian referendum on leaving the EU if Brussels “fails to refocus on its original role as an economic and trade alliance” and instead moves towards “political centralisation.”

Considerable tension exists between Member States and the EU over the EU’s role as a guarantor of fundamental rights. This is clear in Germany as well as in Britain.

---

396 Ibid.
398 Kate Lyons and Gordon Darroch “Frexit, Nexit or Oexit? Who will be next to leave the EU” (27 June 2016) The Guardian <www.theguardian.com>.
following their recent move to reject the supremacy of EU law. If further Member States follow Brexit there could be a substantial withering of the authority of EU law.

The development of fundamental rights and the Charter within the EU could conceivably take on as much significance as the United States Bill of Rights, it could be a defining feature of the EU’s development as a polity.\textsuperscript{399} However the realisation of that goal appears challenging in light of the tensions discussed above.

Adequacy intends to propagate high EU standards of data protection, built on fundamental rights. That campaign is significantly curtailed if the fundamental rights foundation on which adequacy is built is challenged and the EU loses the support of its Member States.

\textit{C Key Points}

Adequacy requires, by reason of international commitments or domestic law, adequate protection of the private lives and basic freedoms and rights of individuals.

Adequacy is constructed on a foundation of fundamental rights. Therefore the fundamental rights jurisprudence of the ECJ is crucial for understanding the requirements of adequacy.

Whilst the ECJ is a relatively new court, with limited case law on data protection and privacy, it has benefitted from the experience and expertise of the ECtHR.

Nevertheless the ECJ has had difficulty defining the scope and shape of the rights to data protection and privacy under the Charter. The rights are often combined together and the relationship between them is unclear.

There is little authority for the protection provided by art 8 of the Charter and it has limited current utility as a sui generis right.

\textsuperscript{399} Douglas-Scott, above n 365, at 655.
Schrems failed to clarify the nature of the rights as the ECJ did not undertake a thorough analysis of the fundamental rights requirements of adequacy—instead finding the Safe Harbour invalid on a narrow technical point.

PNR agreements found to provide adequate protection were another missed opportunity to clarify the role of fundamental rights protecting against intrusions justified on national security grounds.

Following an unsettling pattern, the ECJ found the first PNR agreement invalid for technical competence issues rather than a lack of fundamental rights protection. This has eased the introduction of later PNR agreements.

The PNR agreements and Safe Harbour are evidence the ECJ has pursued economic and political ties with the United States ahead of the fundamental rights of European data subjects.

There is a broad concern the EU’s centre of gravity lies in the economy rather than in fundamental rights. This claim draws on: the history of the EU as an economic institution; the equating of economic rights with traditional human rights; and the ability of economic interests to shape fundamental rights over the long term through lobbying and litigation.

Additionally the EU may be asserting fundamental rights as instruments for achieving primacy and autonomy, rather than as goods in themselves. This criticism is given weight by the expansion of EU competence over its history and the tensions between Member States and the EU, as well as between the EU and other supranational bodies such as the UN.

These tensions have produced cracks in the fundamental rights authority of the EU with some Member States challenging the EU’s authority and others looking to leave the EU itself.

Ultimately fundamental rights in the EU provide an unclear and possibly unstable foundation on which to uphold the requirements of adequacy.
The EU is looking to protect personal data with: (i) the Regulation, which will replace the Directive; and (ii) the Privacy Shield, which will replace the Safe Harbour. Both have significant consequences for the shaping of adequacy.

**A The General Data Protection Regulation**

The Regulation will come into force in May 2018. According to the European Commission the Regulation will deepen the EU internal market, streamline international transfers of personal data, ensure stronger enforcement of data protection rules and set global data protection standards. However the architecture of transborder flows and adequacy decisions remains essentially the same.

The Regulation has a more detailed catalogue of the elements required for adequacy and has formally adopted the standard of “essential equivalence” of fundamental rights protection as required by Schrems.

The specific areas for adequacy analysis under art 45(2) include:

(i) the rule of law;
(ii) respect for human rights and fundamental freedoms;
(iii) legislation concerning public security, national security, criminal law and access of public authorities to personal data;
(iv) implementation of that legislation;
(v) data protection rules and case law;
(vi) effective and enforceable data subject rights and effective administrative and judicial redress for data subjects;
(vii) whether there is an independent supervisory authority in the third country which can assist and advise data subjects on their rights and can cooperate with

---

401 At 6.
402 Recital 104.
the EU supervisory authorities; and
(viii) the international commitments, obligations and organisations the third
country has entered into, particularly relating to the protection of data.

In light of the new provisions in the Regulation the level of personal data protection
required for adequacy is increased. For example: there is a new right for data
subjects to request data erasure\textsuperscript{403} (the right to be forgotten); data controllers will
have to notify both data subjects and the supervisory authority in the case of a data
breach;\textsuperscript{404} there is a right to data portability which allows data subjects to access
and transfer their personal data across different services; special protection for
children;\textsuperscript{405} fines for non-compliance are available, up to EUR 10,000,000 or 2 per
cent of the corporation’s annual turnover, whichever is highest;\textsuperscript{406} a right to
explanation of algorithmic decisions is introduced;\textsuperscript{407} and there is a new
requirement for data protection by design and by default.\textsuperscript{408}

The Regulation looks to reduce compliance costs by removing the general
notification requirement for transborder processing however new obligations
would appear to offset these savings. Notably the requirements for data protection
impact assessments, the documenting of all processing operations in detail and
notification to data subjects and National Supervisory Authorities in the event of a
security breach will all increase compliance costs- although they could be expected
to increase the standard of protection.\textsuperscript{409} The notification requirements for
transborder processing under the Directive were severely under enforced so the
removal of the requirement is pragmatic. For example in 2007 the Spanish Data
Protection Authority received notification for just under 8,500 international data
transfers. If all were reported as required the number would likely be in the millions
or even billions.\textsuperscript{410}

\textsuperscript{403} Art 17.
\textsuperscript{404} Art 33 and 34.
\textsuperscript{405} Art 8.
\textsuperscript{406} Art 83.
\textsuperscript{407} Art 13(2)(f), Art 14(2)(g).
\textsuperscript{408} Art 25.
\textsuperscript{409} Bygrave, above n 1, at 177.
\textsuperscript{410} Kuner, above n 3, at 144.
Under the Regulation the European Commission is expected to review adequacy decisions at least every four years and monitor developments which might affect adequacy decisions.\textsuperscript{411} Additionally the European Commission and the National Supervisory Authorities are required to “engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data.”\textsuperscript{412} Scepticism may be appropriate in this context given Member States and the European Commission were supposed to inform each other under the Directive if they considered a third country was not ensuring an adequate level of protection.\textsuperscript{413} After the Snowden revelations, it became apparent New Zealand and Canada, both with positive adequacy decisions, were complicit in mass surveillance as part of the Five Eyes surveillance alliance however neither lost their adequacy status. Although the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs called on both the Commission and Member States to assess whether the protection provided by New Zealand and Canada was still adequate no further action appears to have been taken.\textsuperscript{414}

Looking internally the EU’s criticism of United States mass surveillance is duplicitous in light of mass surveillance by Member States. Crucially the United Kingdom is involved in Five Eyes. Additionally the Netherlands, France and Denmark are involved in Nine Eyes and Germany, Belgium, Italy, Sweden and Spain are involved in Fourteen Eyes. The European Parliament has called on those involved to revise their intelligence operations so they are in line with European fundamental rights obligations, as well as the principles of necessity, legality, proportionality, due process, notification, transparency and the presumption of innocence.\textsuperscript{415} However there has been no action taken against complicit Member States. The Regulation loses moral force to set high benchmarks for fundamental

\textsuperscript{411} Art 45(3)-(4).
\textsuperscript{412} Art 50(c).
\textsuperscript{413} Art 25(3)
\textsuperscript{414} Claude Moraes “Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs” (Report for the Committee on Civil Liberties, Justice and Home Affairs, 2013/2188 (INI) A700139/2014, 21 February 2014) at 45.
\textsuperscript{415} At 21.
rights protections when some of its largest countries are themselves complicit in
generalised mass surveillance.

Counterintuitively the increases in protection from data portability, privacy by
design and default and the right to an explanation may make adequacy less effective. Very few countries have achieved adequate protection and by raising the bar and requiring regular reviews those that have may fall out of favour. Moreover there may be weak incentives for other countries to apply—especially given BCRs and MCMs allow data to flow outside of a formal adequacy decision. It is noteworthy the Art 29 WP conceded in 1998 that the adequacy decision project would be less effective if relatively few countries achieved positive adequacy findings.\textsuperscript{416} Only twelve countries have received adequacy decisions and a number are minor players in the global data processing environment, including Andorra, Guernsey, the Faeroe Islands, Jersey, Israel and the Isle of Man. Clearly the standard is either seen as too high for many countries or they do not see a positive adequacy decision as having great utility.

Nevertheless the new requirements of the Regulation do contain some innovative features to improve privacy and the level of protection afforded by adequacy. I will examine three of the new provisions—the right to data portability, the right to an explanation and privacy by design and default.

1 \textit{Right to data portability}

The right to data portability, whilst not directly improving data protection for data subjects, could have a positive indirect effect. The right could achieve this by increasing the ability of smaller firms to compete against firms with market dominance.

Increasing the competitiveness of online markets gives legitimacy to the neoclassical position that the market will incentivise data controllers to protect personal data as otherwise data subjects will change providers. This argument is

\textsuperscript{416} Article 29 Working Party, above n 143, at 26.
false if data subjects have no meaningful alternatives but a market based solution gains credibility to the extent competition is increased. Issues of imperfect information and unequal bargaining power might remain, however increased competition from data portability could be instrumental in incentivising corporations to raise their data protection standards.

The right can reduce monopolisation in online markets by significantly reducing the switching costs of changing provider. Unlike traditional markets, the degree of competition present in online markets is often determined by network effects and switching costs.\textsuperscript{417} Switching costs are impediments to users changing their service provider- they can be financial such as cancellation costs or effort based such as having to learn to use new software or re-uploading many photos to a new social media website. Network effects on the other hand concern the extent to which a user’s utility from a service increases as the number of other users increases. For example Facebook becomes increasingly valuable to users as more people join the website as the possibility of communicating with valued people increases.\textsuperscript{418} Likewise LinkedIn becomes more valuable to its users as more people join as it increases the possibility of making professional connections.

High switching costs and network effects can concentrate market dominance over time. This can be an issue for data protection standards if the dominant firms do not adopt high standards and data subjects do not have meaningful alternatives. For example Facebook enjoys substantial market dominance in the social network market, giving the corporation significant power to shape privacy and data protection norms. This is concerning given Facebook’s privacy failings and Mark Zuckerberg’s assertion that privacy is no longer a social norm.\textsuperscript{419} If Facebook has to allow its users to easily transfer their data to another social media website this


\textsuperscript{418} Justus Haucap and Ulrich Heimeshoff “Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization?” (Discussion paper for Düsseldorf Institute for Competition Economics, Düsseldorf, January 2013) at 3.

\textsuperscript{419} Johnson, above n 114.
encourages other firms to compete against Facebook, hopefully giving data subjects greater choice to select a corporation with their desired level of privacy safeguards.

2 Right to an explanation

The newly styled right to an explanation of algorithms could reduce discrimination and significantly improve transparency for data subjects. However it requires a dramatic overhaul of current algorithm practices and as the first piece of legislation to explicitly address algorithmic accountability its success or failure will reverberate well beyond Europe.

First, the right looks to reduce discrimination through data sanitation. This occurs by disallowing sensitive data- revealing racial and ethnic origin as well as other special categories- from being the basis of automatic decisions producing significant legal effects. However true data sanitation is frustratingly difficult to achieve as removing categories may not affect bias as the relationship between the special categories and the outcome can be embedded in proxy variables. For example home address, with other factors, could be a proxy for ethnicity. Removing the special categories may simply deepen the bias making it more difficult to detect.

Second, the right provides transparency by entitling data subjects to “meaningful information about the logic involved” as well as the consequences of algorithmic decisions. However beyond intentional secrecy to protect trade secrets there is a subtle ancillary issue. Companies may not know exactly how their self-learning algorithms are making decisions. The algorithms can become less transparent over time as different programmers leave and join the programming team. Additionally the algorithms can self-learn and evolve. This can make it difficult to understand where bias may be coming from. For example consider the google advertisements suggesting criminal background checks for “black sounding” names, unrelated to arrest records. The Google algorithm learns over time which advertisements get the

---

421 At 3.
422 Regulation, art 13(2)(f), art 14(2)(g).
most clicks out of several possible for a given search string. The discrimination could therefore be from the algorithm responding to external data- biased clicking by society- or it could be embedded in the algorithm itself. The architecture of self-learning algorithms provides exceptional flexibility in their development but makes their internal logical elusive.

The right to explanation is likely to be particularly difficult to achieve when discrimination is unintentional and opaque, in that it cannot be determined *a priori*. How to achieve the specificity required by the right to explanation may prove to be an incredibly nuanced and difficult task. Some commentators such as Professor Nicholas Diakopoulos argue transparency through traditional mechanisms of access requests and disclosure is likely to be insufficient.

A new approach- algorithmic accountability reporting- may provide a partial solution for Member States and countries looking to achieve adequacy. Just as corporations require accounting auditing, they could also be required to undergo algorithm auditing. Effectively it would involve reverse engineering- varying inputs and comparing outputs to make intuitions about the underlying algorithms. Harvard Professor Latanya Sweeney followed this process to discover the criminal background check bias mentioned earlier. Nevertheless, although she could identify the bias she could not decipher where it was coming from. It is a complex area with many unknowns and no conventional approach although it has proved successful in identifying, if not explaining, algorithmic discrimination in interest rates and pricing.

The Regulation does not specifically provide for algorithm audits however they could become an important component of Data Impact Assessments under art 24, a component of industry based Codes of Conduct analysis under art 40 or a component of Certification under art 42. Unfortunately algorithmic auditing in the United States likely breaches the Computer Fraud and Abuse Act as the testing

---

423 Sweeney, above 299, at 34.
424 Goodman, above n 420, at 3.
426 Goodman, above n 420, at 4.
usually requires violating the common terms of service of common websites.\textsuperscript{427} However there is a current case brought by the American Civil Liberties Union challenging the constitutionality of the Act to allow academic researchers to test internet algorithms in the context of identifying racial discrimination.\textsuperscript{428}

It is unclear who could provide the external auditing in an EU context- a for profit certification company, a quasi-public corporation or a public sector body. Certainly it would require significant resources and technical expertise largely outside of the skill set of the European Supervisory authorities. Ultimately the introduction of the right to explanation has tremendous promise however the implementation in practice is likely to be incredibly difficult and resource intensive if it is to be effective.

3 Privacy by design and default

Privacy by design and default involves imbedding privacy into the design of the cyber architecture- preventative, proactive protection rather than remedial, reactive protection. The Regulation does not provide a detailed explanation of the principle however pseudonymisation is explicitly referred to.\textsuperscript{429}

Privacy by design and default is a shift to the technology itself protecting privacy. Consider location data, it can provide a detailed picture of a data subject- inferences can be made about where the data subject lives, works, eats and goes to the doctor. Health information can also be inferred from walking speed and frequency of fast food visits. As Big Data continues to develop so too will the inferences from location data. Many applications use location data to function, for example weather report applications. These applications could implement privacy by design and default by receiving a course location only. Instead of tracking the data subject to a few metres

\textsuperscript{427} 18 USC § 1030
\textsuperscript{428} “Sandvig v Lynch- Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online” (29 June 2016) American Civil Liberties Union <www.aclu.org>.
\textsuperscript{429} Art 25(1)
the application could be designed to give a location to the nearest twenty kilometres- sacrificing minimal functionality for significant privacy gains.\textsuperscript{430}

Additionally when computers crash often data are collected for troubleshooting and diagnostics. If the crashes occur a few weeks apart the crashes are often unconnected, however if they occur a few hours apart then the first crash is more likely to be relevant for diagnosing the second. Consequently the troubleshooting application could be designed to change the computer's unique identifier every day. In this way the application does not gain a long record about a single user but can still link crashes to each other if they occur in a similar time frame.\textsuperscript{431} This protects the user's computer habits whilst still providing the troubleshooting application with sufficient data for diagnostics.

Privacy by design and default can be an effective tool for protecting data subjects, particular those who are unsophisticated or young. However the focus in the Regulation on pseudonymisation and anonymisation is incredibly concerning.\textsuperscript{432} Reidentification of pseudonymised or anonymised data will continue to occur-particularly as hardware power and the richness of auxiliary information increase as discussed in section II(C)(2). This reidentification can produce significant privacy harms yet the anonymised data flows will not engage the requirements of the Regulation or adequacy. Privacy by design and default needs to have a much broader scope than anonymisation if it is to be effective.

There is a fundamental accretion problem where intermediary reidentification steps can breed further success. Professors Narayanan and Schmatikov outline that any supposedly benign link between deidentified data is an issue as it reduces information entropy- shortening the inference chain required to connect a data subject from a given fact.\textsuperscript{433} Linking pseudonymised user records between Netflix ratings and IMDb databases may appear benign however further inferences can often be made. Perhaps if a data subject reused their username on another website

\textsuperscript{431} Ibid.
\textsuperscript{432} Recital 26.
\textsuperscript{433} Ohm, above n 102, at 1746.
they could be linked to a Facebook profile, an online victim's support community, or a website indulging indecorous tastes.434

Privacy by design and default has the potential to significantly increase the requirements of adequate protection however it will require a broader implementation than the anonymisation and pseudonymisation suggested by the Regulation.

B The Privacy Shield

The Privacy Shield435 is the intended replacement to the Safe Harbour. The agreement was reached on the 2nd of February 2016 and represents the new framework for transborder data flows between the EU and the United States.436 The European Commission believes it will strengthen fundamental rights and restore Europeans’ trust in the digital economy.437

The Privacy Shield intends to provide legal certainty for companies and “inject new momentum into the transatlantic partnership.”438 As part of this relationship, the Commission has stressed how the EU and the United States share common values, political and economic objectives and will “cooperate closely in the fight against common threats to our security.”439 This is a slightly forced narrative given the differences across the Atlantic in how privacy is conceptualised.

Enthusiasm for the scheme is not widespread and controversy surrounds its implementation. Crucially the Art 29 WP has completed an examination of the protection provided by the Privacy Shield and has significant concerns not shared by the European Commission.

The European Commission has praised some of the proposed benefits to the Privacy Shield including a new Ombudsman who will work with EU data subjects to check

434 At 1747.
436 Commission of the European Communities, above n 400, at 3.
437 At 3.
438 At 8.
439 At 2.
whether relevant national security laws have been complied with.\textsuperscript{440} Additionally the European Commission has commended the passing of the United States Freedom Act which allegedly strengthens judicial oversight of mass surveillance and increases public transparency.\textsuperscript{441} This is a curious commendation given the position in EU law that generalised surveillance is illegal, regardless of whether there is oversight. However the Judicial Redress Act of 2015 has usefully extended the privacy protections available under the Privacy Act of 1974 to European citizens.

From a dispute resolution perspective the Privacy Shield Panel establishes a new, last resort mechanism which can take binding action against companies operating under the Privacy Shield.\textsuperscript{442} Whilst the new avenues for redress, including the Ombudsman and Privacy Shield Panel, represent a deployment of resources to data protection enforcement, which is encouraging, the Art 29 WP is concerned they may be too complex and ineffective in practice for European data subjects.\textsuperscript{443} Additionally there is concern the Ombudsman is not sufficiently independent for the requirements of EU law and has inadequate powers to fulfil its enforcement duties.\textsuperscript{444}

Disappointingly the Art 29 WP found the Privacy Shield, whilst an improvement over the Safe Harbour, lacks some key data protection principles required by EU law. For example the data retention principle was found to be ineffectively provided for by the Privacy Shield’s Purpose Limitation and Data Integrity principles. The Art 29 WP is also concerned there is no requirement to delete data after the purpose for which it is processed has become obsolete.\textsuperscript{445} Additionally the specific protections against decisions based on automated means are unclear.\textsuperscript{446} This issue is likely to compound as the prevalence of algorithm based decision making continues to flourish.

\textsuperscript{440} At 9.
\textsuperscript{441} At 4.
\textsuperscript{442} At 10.
\textsuperscript{443} At 3.
\textsuperscript{444} At 3.
\textsuperscript{445} At 17.
\textsuperscript{446} At 3.
There is also concern the nomenclature employed by the Privacy Shield is inconsistent and results in lacunas of protection. For example the principles are applicable when an organisation “stores, uses or discloses” personal data as opposed to the standard trigger of “processing.” This introduces uncertainty over whether components of processing such as collecting and deleting, which might not be contained in “stores, uses or discloses,” engage the obligations and liabilities of the scheme. Additionally whilst the scheme defines personal data as “data about an identified or identifiable individual,” for human resources data the principles only apply to “identified records” which appears to exclude the broader “identifiable” trigger. Overall the framework was found to have a considerable lack of clarity.

Annex VI to the Privacy Shield, a letter from the Office of the Director of National Intelligence, also provokes considerable concern. The Annex holds “Intelligence Community elements must collect bulk signals intelligence...to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications.” Annex VI also specifies six purposes for which mass surveillance may take place, being: detecting and countering certain activities of foreign powers; counter-proliferation; counterterrorism; cybersecurity; detecting and countering threats to United States or allied armed forces; and combating transnational criminal threats. Mass surveillance is incompatible with EU law so it is alarming the Privacy Shield specifically outlines when it may take place. The Art 29 WP did commend the requirement for new adequacy decisions to examine access to personal data by national security and law enforcement agencies however this is little consolation if mass surveillance is allowed.

Contrary to the assertions of the European Commission, considerable uncertainty remains over how the Privacy Shield will cope with the new standards of the Regulation. The Art 29 WP is particularly concerned with the impact of the right to

---

447 Privacy Shield, Annex II(1)(III)(6)(f) and Annex II(1)(8)(a).
449 At 2.
450 Annex VI(b).
451 Ibid.
data portability and privacy by design and default, which are not included in the Privacy Shield. Given how significant the additions are it is short sighted for the Privacy Shield to not address the new provisions. If the Privacy Shield does not implement the new standards then it will be more likely to be successfully challenged in the ECJ.

If the Privacy Shield fails to attract businesses or is challenged in the ECJ it is probable that MCMs and BCRs will have to provide the legal mechanism for transborder flows between the United States and the EU. MCMs and BCRs are less desirable than full adequacy decisions as they create pockets of adequacy rather than securing a high level of protection throughout a full sector or country. Whilst they still provide adequate protection their narrowness makes them less efficient at spreading EU norms and they will likely require updating in light of the new requirements of the Regulation.

Max Schrems has described the Privacy Shield as “ten layers of lipstick on a pig” and has indicated he and others are likely to challenge the Privacy Shield’s legality. Additionally the National Supervisory Authorities are, under the Regulation, expressly given the power to suspend data flows to recipients in third countries. This fractures the legal certainty for corporations looking for a continuous transfer of data through the Privacy Shield. Pro-privacy National Supervisory Authorities and groups such as Facebook-v-Europe could attack the Privacy Shield and prevent the data flows-especially in light of the violation to fundamental rights entailed by mass surveillance. Businesses will be unlikely to utilise the scheme if they believe it may be challenged and struck down. Ultimately the Privacy Shield must be seen as failing both its purposes-the promoting of the digital economy and the protection of fundamental rights. It does not constitute adequate protection.

---

452 Article 29 Working Party, above n 448, at 15.
454 Art 58(2)(j).
IX WHERE TO FROM HERE?

This thesis opened with an account of how privacy was conceptualised in Europe and the United States. Optimistically I thought public opinion on mass surveillance could shift if the pro-privacy narrative could be massaged for each audience: for the United States- mass surveillance is an invasion into the private home and space by public authorities; for Europe- mass surveillance is an affront to personal dignity and autonomy. From this public opinion shift I thought pressure could be applied to legislatures to improve the standard and enforcement of adequate protection. However with the misperceptions of the benefits of mass surveillance and the overestimation of the terrorism harms I do not think public discourse will catalyse change in the short or medium term.

The law is responding to perceptions of insecurity and public expectations of strong action against terrorism. Most of society relies on intuitive risk assessments where experience with unusual hazards comes from the news media which is problematic as there is a media fixation with horrific, unexpected crimes rather than mundane issues producing significantly greater harm. Such is the frenzied terrorism coverage that repeated media exposure to the Boston Marathon bombings was associated with higher acute stress than direct exposure-being at or near the bombsite when the explosion occurred.

Humans are ineffective at analysing the difference between a one in a million and a one in a thousand chance event. The inaccurate risk perception is amplified when there is a perceived lack of control, inequitable distribution of the risk and fatal consequences in the event the risk materialises. It is a sad point that two days after the Boston Marathon bombing a fertiliser plant in Texas exploded killing five times as many people as died in Boston. The official investigation found the explosion “resulted from the failure of a company to take the necessary steps to

---

456 Alison Holman, Dana Garfin and Roxane Silver “Media’s role in broadcasting acute stress following the Boston Marathon bombings” 111 PNAS 93 at 93.
457 Slovic, above n 455, at 283.
Avert a preventable fire and explosion.\textsuperscript{458} In 2015 work injuries in the United States resulted in more deaths than the equivalent of 1600 Boston Marathon bombings.\textsuperscript{459} Legislation and political attention are following perceptions of harm rather than harm itself.

As a partial solution I propose shifting the locus of discussion from mass surveillance and national security to data security. Data security concerns unauthorised destruction, alteration and disclosure of data as well as unauthorised access, including failing to gain explicit unambiguous consent. Moving the debate to the harms of data insecurity shifts the focus from terrorism issues to the economic and privacy costs of failing to secure data. The Regulation could play a strong role in raising data security through the requirements of the new provisions of the Regulation as well as through adequacy decisions.

This new focus could indirectly undermine mass surveillance and appeal to corporations looking to reduce the costs of data insecurity. Professor Rascoff makes an important point when he notes ambition can be made to counteract ambition-technology firms pursuing their own interests can pressure the government to push back against a culture of surveillance. As American Civil Liberties Union lawyer Ben Wizner notes, “one of the great contributions that Snowden has made is to make some very powerful tech companies adverse to governments.”\textsuperscript{460} Technology companies could be encouraged by the Regulation’s provisions to design products and services with inbuilt protections for data security, making mass surveillance more difficult to undertake.

A push for higher standards of data security is likely to be much more successful if it is presented in the interests of corporations as well as data subjects. Rascoff notes that although the corporate motivations for privacy may be “shallow” and “malleable,” in that they are economically driven, he notes the Snowden leaks have

\textsuperscript{458} “Chemical Safety Board Ongoing Investigation Emphasizes Lack of Protection for Communities at Risk from Ammonium Nitrate Storage Facilities; Finds Lack of Regulation at All Levels of Government” (22 April 2014) United States Chemical Safety Board <www.csb.org.gov>.
\textsuperscript{460} Rascoff, above n 326, at 689.
“galvanised technology firms and allies to join longstanding sceptics of the surveillance state in putting pressure on the White House to resist the agenda of the intelligence bureaucracy.” NSA Director Admiral Michael Rogers, who also serves as Commander of the United States Cyber Command and Chief of Central Security Service, has noted the working relationship between some telecommunications and technology companies with the NSA may never return to what is was before Snowden’s leaks.

Whilst mass surveillance and national security are divisive issues, there is considerable public support for increased data security. Recent research by the Pew Research Centre shows the majority of United States citizens do not trust federal government and social media sites to protect their personal information. Indeed 64 per cent of United States citizens are aware they have personally experienced a major personal data breach and over 40 per cent have experienced fraudulent charges on their credit cards.

A recent survey requested by the Director General for Home Affairs of the European Commission shows substantial concern over data security also exists in the EU. Of the total respondents: 73 per cent were concerned their online personal information was not being kept secure by websites; 67 per cent were concerned their personal information was not being kept secure by public authorities; 89 per cent tried to avoid disclosing personal information online; and 85 per cent believed the risk of becoming a victim of cybercrime was increasing. In response to these beliefs the Regulation could set high standards for data security and require countries seeking adequacy decisions to reach these new standards. Whilst there has been political benefits to appearing tough on national security and terrorists, improving data security could be also be an incredibly popular political policy.

---

461 At 668.
462 At 663.
463 Kenneth Olmstead and Aaron Smith “Americans and Cybersecurity: Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives” (26 January 2017) Pew Research Centre <www.pewinternet.org>.
Widespread mistrust of data security could also catalyse data protection improvements by corporations looking to satisfy consumer demand, independent of political or regulatory pressure. However corporations are not homogenous. Some, such as Apple, receive a benefit from producing smartphones with high data protection standards. However others, such as Facebook, might lose revenue from greater data protection. For example if internet browsers automatically delete cookies before accessing Facebook, Facebook's ability to sell targeted advertisements will be reduced. As a consequence of the heterogeneous nature of data controllers, regulatory action rather than market mechanisms are likely to be more effective at achieving widespread improvements.

However there is an encouraging rise in the marketing of technological products resistant to data breaches and mass surveillance.\textsuperscript{465} This is a crucial change in consumer tastes. Rather than seeking data havens in a race to the bottom of data protection law, corporations may produce products and seek environments with high data protection to build trust in their businesses.\textsuperscript{466} Progressively more companies are also increasing financial and human resources to comply with data protection law and many are appointing specific data protection officers.\textsuperscript{467} Given the rise in value of data, operating in countries or sectors with improved data protection can increase firms' reputations - business are increasingly aware of the negative publicity, legal expenses and loss of business following data breaches.

Before looking at the specific solutions which could be implemented through the requirements of the Regulation and adequacy I will canvass what is at stake with data insecurity - the harms to individuals, businesses and governments if low levels of data security persist. In particular intellectual privacy, discrimination and cybercrimes will be examined.

\textsuperscript{465} Rascoff, above n 326, at 664.
\textsuperscript{466} Kuner, above n 3, at 104.
\textsuperscript{467} At 150.
A Harms of Data Insecurity

Data insecurity can threaten innovation by undermining the environment in which it flourishes- protected spaces where orthodoxies can be tackled and tinkered with. Professor Neil Richards uses the concept of “intellectual privacy.” It refers to the protected space in which ideas are created, debated, reworked and refined. Richards believes intellectual privacy allows experimentation with controversial and deviant ideas which can precipitate cultural and economic advance. However this project can be undermined by data insecurity. If people believe their unfinished beliefs and intellectual experiments can be watched and exposed then there is a chilling preference for the mainstream and accepted rather than the bold and controversial.

As Professor Julie Cohen notes a society will “dampen and modulate behavioural variability” if it has “unchecked ascendancy of surveillance structures.” She believes such surveillance makes it impossible to maintain a “vibrant tradition of cultural and technical innovation.” Individuals may be less likely to engage with unpopular ideas or analyse controversial books and videos for fear of being profiled in a certain way. From a personal perspective I have certainly considered how my researching of terrorist attacks for this thesis could alter my online profile.

Problematically data insecurity can also promote discrimination, by giving data controllers an increasing amount of data about data subjects. The personal data can be gained by tracking not explicitly consented to or even from illegally obtained databases of individuals exhibiting certain behaviours- such as online gambling. Treating different categories of people differently can appeal in some contexts, such as providing discounts to repeat customers. However other methods such as those employed by Target are less comfortable. By mining the data trail of shoppers Target could make inferences about whether or not a data subject was pregnant and market to them accordingly. Big Data analysts from Target admitted to targeting individuals experiencing the “chaotic exhaustion that accompanies the birth of a child” on the

---

469 Julie Cohen “What Privacy is For” 126 Harvard Law Rev 1904 at 1918.
basis that if they “buy diapers from us, they’re going to start buying everything else too.”

Commercial surveillance of data trails can track customers across the internet, allowing corporate interests to identify and nudge data subjects in positions of relative weakness. This has largely been through internet browsing on personal computers and smartphones however the "Internet of Things," where appliances, cars and homes increasingly process personal data, will reduce the sphere of unobserved activity. Knowing when an individual is vulnerable and experiencing the vicissitudes of life allows corporations to manipulate and discriminate. Improved data security could reduce the amount of data available to data controllers and hence reduce the opportunities for discrimination.

Blackmail is also a risk raised by data insecurity and can be perpetrated by both private and state actors. Gathering information for blackmail purposes has traditionally been costly, such as the extensive resources expended following Martin Luther King Jr and installing listening devices in his hotel rooms. However in the internet era a huge portion of society are relatively low cost potential targets.

Leaked documents from Edward Snowden about the operations of the Joint Threat Research Intelligence Group at the Government Communications Headquarters (GCHQ) in the United Kingdom are particularly alarming. Individuals and corporations have been blackmailed and manipulated by the taskforce. Under the taskforce’s instructions confidential information can be hacked then leaked, false material can be posted and attributed to the target, personal computers can be shut down, fake victim blog posts can be circulated and fake communications can be made to colleagues, neighbours, friends and business partners. Distressingly, the targets include people neither charged nor convicted of crimes, and include those merely suspected of online protest activity. These are incredible powers for a government to have. Improved data security could make these attacks more difficult.

---

470 Richards, above n 476, at 1939.
471 At 1940.
472 At 1943.
and expensive to carry out although it might be impossible to completely defend against them.

From a commercial perspective, a recent study estimated cybercrime in the year ending September 2015 cost the EU USD 62,000,000,000, North America USD 61,000,000,000 and Asia Pacific USD 81,000,000,000. However this may be a conservative estimate. Other reports expect annual data breaches to cost over USD 2,000,000,000,000 globally by 2019. The World Economic Forum notes a significant portion of cybercrime is unobserved—particularly corporate espionage where unauthorised access to confidential data is difficult to detect. However large scale cyber-attacks are continuing to enter the public discourse, such as Yahoo having over 1,000,000,000 user accounts compromised in August of 2013.

It is worth noting governments also gain from raising their data security standards. There have been significant cybercrimes committed against public bodies. For example in 2015 the United States government agency in charge of background checks suffered a data breach. Names, addresses, family information, financial information, health information and social security information of more than 22,000,000 federal workers were stolen. The background checks were required for intelligence and military officers to get secret and top secret clearances. More than a 1,000,000 fingerprints were also taken.

In 2014 the White House network was breached and the president’s schedule and emails were obtained. Additionally John Brennan, director of the Central Intelligence Agency, had his personal email compromised, allegedly by a high school

---

476 Ibid.
student. Brennan’s emails contained sensitive documents including the questionnaire he filled in to receive his security clearance.\textsuperscript{479}

Former President Barack Obama even described cyber insecurity as “one of the most serious economic and national security challenges [the United States] face as a nation.”\textsuperscript{480} General Keith Alexander, former Director of the National Security Agency and Commander of the United States Cyber Command boldly went on record holding the United States ability to respond to a major cyber-attack as around a three out of ten.\textsuperscript{481}

Recently data insecurity has been firmly in the public national security discourse in the United States. Throughout the lead up to the 2016 United States election Hilary Clinton was severely criticised for using a private email server to handle classified, secret and top secret information.\textsuperscript{482} There is serious concern the server was not adequately protected from foreign agencies.

Developing better data security for the public sector mitigates against these harms. However improved data security generally also benefits governments as it reduces the threat of bot net attacks. For example the cyber-attack on Estonia in 2007 which shut down banks, government communications and online media for around two weeks was conducted by a network of compromised computers controlled by attackers.\textsuperscript{483} If the standards of data security are raised across all of the European Economic Area, as well as internationally though adequacy, then this would reduce the efficacy of bot net attacks.

Disappointingly governments may taper their enthusiasm for improved data security as new standards could undermine their ability to conduct mass surveillance. Nevertheless there are substantial economic and fundamental rights

\textsuperscript{479} Ibid.
\textsuperscript{480} Martha Finnemore and Duncan Hollis “Constructing Norms for Global Cybersecurity” (2016) 110(3) American Journal of International Law 425 at 453.
\textsuperscript{483} Finnemore and Hollis, above 490, at 453.
benefits flowing from greater data security which could catalyse reform and gain support from the private sector. Crucially the emotionally charged debate over whether mass surveillance is necessary and proportionate to modern national security threats could be replaced by a pro-privacy and anti-cybercrime data security conversation.

**B Why Can Adequacy and the Regulation Assist?**

Art 25 of the Regulation requires, considering the nature, context, scope and purposes of processing, as well as the state of the art and cost of implementation, and risk of fundamental rights infringements, that the data controller and processor take appropriate technical and organisational measures to protect data by design and default. Additionally art 32(1) requires appropriate technical and organisational measures to be taken to ensure a level of security appropriate to the risks of processing.

These articles provide a framework for a higher level of adequate protection through improved standards of data security. Nevertheless art 17 of the Directive required such technical and organisation measures to protect personal data but diverse measures were taken by different Member States resulting in varying protection. To provide harmonisation in the case of the Regulation, specific measures for achieving data security could be required rather than simply setting the goal of appropriate data security.

Some may argue the market itself will appropriately respond to consumer demand for increased security. However Professor Ross Anderson believes a microeconomic analysis can challenge this position with perverse incentives, asymmetric information, liability dumping and externalities undermining data security in an unregulated market.

Problems arise when a party in a position to secure a system is not the same party as the one who would suffer a security breach. For example in the United Kingdom

---

484 Art 25(1)
485 Kuner, above n 136, at 289-290
and Norway, the burden of proof in fraud against autoteller machines lies with the customer. On the contrary in the United States the burden falls with the bank. Unsurprisingly the banks in the United Kingdom and Norway were less effective in securing their systems against fraud.\footnote{Ross Anderson “Why Information Security is Hard- An Economic Perspective” (paper presented at 17\textsuperscript{th} Annual Computer Security Applications Conference, Louisiana, December 2001) at 1.}

In the case of a data breach, costs can be borne by customers and actors outside the attacked company. As a consequence a company may underinvest in the level of protection that is efficient from a societal viewpoint even if they have invested sufficiently to manage their internal exposure.\footnote{Nathan Sales “Regulating Cyber Security” (2013) 107(4) NW U L Rev 1503 at 1507.} For example an energy corporation might not consider the secondary costs borne by their customers in the event of a cyber-attack resulting in a black out. This can result in a level of protection below the societal optimum even if the energy company’s internal cost benefit analysis suggests the protection they have is efficient. This suggests regulating for a higher level of data security could increase total welfare.

Distributed denial of service attacks- mobilising botnets to attack others- provide a sharp display of the Tragedy of the Commons issue. A company or an individual may pay USD 100 for software to prevent their computers from attack, but are unlikely to spend even a fraction of that amount to stop their computers being used as a vector to attack others.\footnote{Ibid.} With cybersecurity, if one firm increases its defences, then that firm is less likely to be a vector for attacks on others and hence the overall security of cyberspace can rise. However cooperation is unlikely without external forces which suggests a strong role for regulatory intervention through adequacy and the Regulation outside of a purely market based solution.

\textbf{C What Specific Improvements Could Be Made?}

The requirement for a level of security appropriate to the risks of processing under art 32(1) refers to Codes of Conduct as a possible mechanism for achieving appropriate data security. The Codes of Conduct could outline specific organisational and technical measures to be taken to meet the requirements of the
Regulation. These measures could also be required for countries applying for adequacy decisions and the standards could be implemented into MCMs and BCRs to give wider penetration for the new, raised protections. I canvass several organisational and technical measures however with resource constraints it may well be the case that only a few are likely to be implemented.

1 Organisational

In order to appropriately mitigate data insecurity the risks needs to be analysed. However they are hard to quantify making it difficult to determine what standards could constitute adequate protection. The risks come in many forms including botnets, exploit kits, spam, identity theft and fraud, social engineering exploits, as well as rogue processors operating outside data controllers’ instructions. Empirical analysis of cybercrime is difficult although it appears to be transitioning from individual specialists committing low volumes of crime to more costly crimes committed by organised groups as well as states.489

Disappointingly a recent Australian survey found 43 per cent of respondents did not report data security incidents, predominantly due to a perception that no benefits would flow from reporting and a fear of negative publicity.490 Additionally a recent United States report estimated only 15 per cent of the nation’s internet fraud victims reported their incidents.491

However compulsory reporting of incidents, funnelled through National Supervisory Authorities to the European Data Protection Board, could be a significant improvement for analysing and responding to the risks of data insecurity. Countries seeking adequacy could be required to join the scheme and those with adequacy could be required to sign up or lose their status. Professor Nathan Sales argues that data breaches could be conceptualised in a similar manner to public

health outbreaks with the collective good benefitting from mandatory timely reporting. They would receive threat reports, analyse the data for broader trends and release recommendations and alerts as required. Some companies might be hesitant to share vulnerability data- weaknesses that can be exploited to access a computer system. However there could be more success focusing on threat data (the types of malware circulating) and countermeasure data (how to prevent and combat infections). Crucially the releasing of statistics and reports by the European Data Protection Board could raise awareness of both the scale of cybercrime and the importance of data security.

This scheme would work well with art 33 and 34 of the Regulation which require the data subject and relevant National Supervisory Authority to be notified when there is a data breach. If the CDC style reporting was not mandatory then there could be self-interested firms who would not submit. This could be dressed as a desire to avoid anti-trust liability but could also be due to reputational concerns or a desire to hold a tactical advantage- particularly if they believed their competitors would be vulnerable. However subsidies, tax credits and intellectual property rights in the cyber security information produced could provide positive incentives. Additionally antitrust liability for exchanged cyber security information could be decided on a rule of reason approach rather than the per se approach.

Threat reporting could operate at a governmental as well as at a corporate level. The European Coal and Steel Community, as the EU was first known, was for the economic benefit of participating Member States. However equally important, the supranational body placed the means of going to war, which at the time were coal and steel, beyond the exclusive control of individual Member States. There is a conceptual equivalence today in sharing cyber-attack and cyber defence data as they

---

492 Sales, above n 487, at 1509.
493 At 1548.
494 At 1546.
495 At 1532.
496 At 1532
497 At 1550.
constitute the means of cyberwar. If governments could be incentivised to participate in the threat sharing scheme then the quality of the threat reports could be expected to sharply rise.

The public is aware of mass surveillance largely through the actions of individuals like Thomas Tamm, Edward Snowden and Chelsea Manning however global surveillance whistle-blowers have been aggressively targeted rather than protected. The European Data Protection Board could develop its own whistle-blower protection mechanism for both Member States and countries applying for adequacy. Whistleblowing mechanisms can be effective tools for rebalancing the information asymmetry between data subjects and controllers and could be a requirement for achieving adequate protection.

Penetration testing could also play a role in improving data security information. It is the legal, authorised location and exploitation of vulnerabilities in computer systems in order to make those systems more secure. It moves beyond simply identification of threats and involves actual proof of concept attacks to prove issues exist. Penetration testing could be encouraged through subsidies, tax and insurance benefits or even required for data controllers in certain industries such as the energy sector. Countries or sectors looking to achieve adequacy could be informed their applications are more likely to be successful with an active penetration testing industry.

The European Data Protection Board could also encourage the legal market for purchasing computer exploits or “bugs,” particularly concerning public sector systems. Firms such as Google and Microsoft pay tens of thousands of dollars in the private sector to individuals and hobbyists who find exploits. There is a thriving black market for these exploits however a legal market, perhaps with reputational awards, could encourage more people to sell their public sector exploits legally. Papers released by Edward Snowden suggest the NSA is spending USD 25,000,000

a year purchasing exploits, the EU could clearly have a purchasing system also.\textsuperscript{500} There could be a requisite membership fee for the scheme, payable by Member States as well as countries looking to achieve adequacy, which could pooled and used to purchase the bugs.

2 Technical

As Professor Joel Reidenberg notes, information policy can be “embedded in network designs and standards”\textsuperscript{501} and Professor Lawrence Lessig famously declared “code is law,” referring to how the architecture of cyberspace, the code, can constrain behaviour.\textsuperscript{502} Their work is at the core of privacy by design and default. Rather than simply requiring the result of security, the Regulation could adopt Spain’s approach of providing specific measures required for achieving adequate protection through code and technical standards. However effective privacy by design and default techniques will differ across industries and contexts. Some baselines such as using up to data antivirus software and firewall protections have widespread application however others such as appropriate storage of biometric data will not. This makes it highly like that whilst certain baselines could be established, a more flexible and effective cyber building code will be sector specific.

Like Lessig and Reidenberg, Professor Neal Katyal, has also argued in favour of minimum standards of data security design in the same way physical structures are subject to building codes.\textsuperscript{503} He draws a parallel between physical space being well lit and cyber space being open source. Just as lighting in physical space allows for more eyes to observe possible crime, open source programs harness a broad range of eyes which can examine code for vulnerabilities and evidence of past attacks.\textsuperscript{504} However observers in cyberspace are not directly analogous to those in real space as only a portion of people can read source code. Katyal concludes that the context is crucial- whilst open source software improves security in many cases, under some

\textsuperscript{500} Mark Ward “How to make money finding bugs in software” (3 February 2014) BBC <www.bbc.com>.
\textsuperscript{501} Kuner, above n 3, at 97.
\textsuperscript{502} Ibid.
\textsuperscript{504} At 2265.
specific conditions involving highly specialised products, it can make it more vulnerable.\footnote{At 2267.} This shows the importance of having flexible codes across different sectors.

Small businesses may require extra assistance to implement data security through privacy by design and default however they should not be exempt from the requirements. As Clay Calvery, director of cybersecurity at a private Virginia firm notes, smaller companies are easier to hack and are increasingly being targeted with ransomware which holds data hostage until money is paid. Indeed by some accounts the majority of all online attacks may be against small and midsize businesses.\footnote{Constance Gustkejan “No Business Too Small to be Hacked” (13 January 2016) New York Times <www.nytimes.com>.}

Encryption is an obvious privacy by design and default technique which could become mandatory for positive adequacy findings. It involves the encoding of data in such a way that it cannot be accessed by anyone other than the party with the appropriate key or password. A study by the Ponemon Institute found it to be a reasonably low cost security measure with a positive return on investment.\footnote{Ponemon Institute “2015 Cost of Cyber Crime Study: Global” (threat report, October 2015) at 6.}

Encryption is not a panacea however as it does not protect against misuse by the recipients who decrypt the data.\footnote{Kuner, above n 3, at 97.}

As discussed earlier coarse location data could also be made mandatory- instead of providing location data to the nearest few metres, new technologies could be redesigned to provide a less specific location, improving privacy without sacrificing efficacy. Location data can significantly reduce information entropy and hence can be instrumental in achieving unauthorised data access.

Another privacy by design and default initiative could be the compulsory storing of biometric identifies in the technology under control of the data subject, such as smart cards or passports.\footnote{Article 29 Working Party and Working Party on Police and Justice “The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data” (02356/09/EN WP 168, Adopted on 01 December 2009).} This would remove the need to host the data in external
databases, such as those held by customs agencies, which if exploited could result in multiple data subjects having their personal data accessed.

The National Supervisory Authorities and the European Data Protection Board would be wise, from a resource point of view, to encourage each sector to have significant participation in the development of the standards for adequate protection as occurred during the refining of the MCMs and BCRs. Other contributors could include the World Wide Web Consortium, an international community dedicated to developing web standards led by Tim Berners-Lee and Jeffrey Jaffe, and the International Telecommunication Union, an agency of the United Nations. The experience of those organisations in developing and coordinating technical standards on a global scale could be useful for the EU in developing data security standards at the EU level.

Tailoring standards for specific sectors would likely be costly however a blanket approach may cause under protection in some sectors and waste resources in others. The health sector for example would likely benefit from a specific code given the particular privacy harms which can flow from health data breaches. For example access control protocols to minimise the number of health care professionals and administrators accessing specific data could be mandatory. Additionally patient names and personal identifiers could be kept separate from health status data as best as possible. As discussed earlier reidentification is still possible given modern techniques however pseudonymisation would make it more difficult.

From an economic perspective critical infrastructure, including the energy sector, healthcare sector, water suppliers, transportation firms and financial service providers would require particularly high standards of privacy by design and default to ensure data security. A retailer operating in a competitive industry is likely to bear most of the cost of a cyber-attack as disappointed customers can take their custom elsewhere.\textsuperscript{510} However a customer living in a certain area may only be served by one utility company. Many critical infrastructure industries such as the telecommunications and energy sector operate in uncompetitive markets with high

\textsuperscript{510} Sales, above n 487, at 1513.
start-up costs which act as significant barriers to entry for new firms. As a consequence many monopolistic, duopolistic and oligopolistic firms in these sectors face limited competition and threat of customer exit. If a power company is the only provider of energy to a town they face reduced incentive to increase cyber security as customers will not be able to quickly and easily redistribute their patronage following an attack. This lack of competition combined with the attraction to criminals of critical infrastructure results in vulnerable underinvestment in cybersecurity.

Critical infrastructure are also vital from a national security perspective. Having the ability to derail a nuclear power plant or cause a water processing plant to produce unsafe drinking water are serious threats. The physical effects flowing from data insecurity can be seen in the damage done to Iran's nuclear program by the incredibly sophisticated Stuxnet worm. It is an uncomfortable thought to consider how many nuclear plants or other critical infrastructure operations might currently be vulnerable to attacks due to low levels of data security.

It is important to note that regulating by design through sector based codes of conduct has significant transparency issues. This is particularly important given one of the core issues of mass surveillance is the lack of debate and normative consensus over its use. When regulation is achieved by code regulatees are denied the ability to make a self-conscious choice over how to act, with the regulators preferring control over autonomy and the moral project of honesty. If all communications are encrypted by default for example, privacy is likely to be improved. However the arguments over why personal data should be protected and the extent to which fundamental rights can be infringed for the pursuit of a public good might slowly be pushed to the background. They are important arguments which need ventilation.

The competing political and legal values embedded in technology can be hidden with certain technological paths seen as natural over time. To mitigate this the European Data Protection Board, National Supervisory Authorities and Code of Conduct

511 Ibid.
contributors would have to protect the deliberative spaces where features of the code could be debated and revised. If elements of the EU cyber building code project were large, open source developments then this would bring the conversation to the public to some extent.

There is an issue the cyber building codes will suffer regulatory disconnect as technologies develop. Drafting the codes in a technologically neutral manner may reduce this disconnect however it would likely come at a cost of specificity. Accordingly the sector based codes will likely have to be living documents, requiring substantial updating as new technologies develop.

Whilst these suggestions for organisational and technical standards for compliance with the Regulation and adequacy require a phenomenal dedication of resources I believe this can be justified. First, by the extent of fundamental rights infringements germinating from data insecurity. Second, and perhaps more pragmatically, by looking at the accelerating financial costs of data insecurity and cybercrime. Thirdly, and indeterminately, by the secret yet undoubtedly significant investment required to develop and maintain the mass surveillance apparatus- funds which should be redirected to data security.
**X CONCLUSION**

Adequacy under the Directive has failed.

Few countries have achieved positive decisions. The Privacy Shield is riddled with uncertainty and expressly permits mass surveillance. The Safe Harbour was found invalid and BCRs and MCMs have been forced to provide small pockets of adequacy for transborder flows to continue.

Fundamental rights to privacy and data protection have been undermined by ineffective enforcement and violated by PRISM. The EU has condemned mass surveillance by the NSA however New Zealand and Canada are also complicit yet maintain their adequacy status. Hypocrisy pervades with Member States themselves participating in mass surveillance.

The EU was well aware of the Safe Harbour’s deficiencies yet it took an underfunded law student to bring the scheme to a conclusion.

The internet remains a surveillance society saturated with commercial and state actors looking to render individuals transparent and predictable through mass surveillance. Adequacy has failed to provide shelter from these forces.

My initial optimism of adequacy under the Directive has been corroded by the political and economic ends dominating privacy concerns. Whilst the European Commission has recently stated “the protection of personal data is non-negotiable in trade agreements” and “European data protection rules cannot be the subject of negotiations in a free trade agreement”\(^{513}\) in the very same document they admit adequacy decisions can “ease trade negotiations.”\(^{514}\) Indeed the “overall political relationship” and “extent of the EU’s (actual or potential) commercial relations....including the existence of a free trade agreement or ongoing negotiations with a third country” are seen as criteria to take into account when deciding which

---

\(^{513}\) Commission of the European Communities, above n 134, at 2 and 6.

\(^{514}\) At 9.
countries an adequacy dialogue should be pursued with. Adequacy is a political and economic bargaining tool. The reality is a commercial one, with Japan and Korea followed by Mercosur currently designated as appropriate targets.

Whilst Schrems is a landmark case it cannot be seen as a strong defence of adequacy. Schrems’ narrow ambit does not provide long term protection against private and public threats. Crucially there was insufficient analysis of the necessity and proportionality of mass surveillance. The essentially equivalent, high level of protection of fundamental rights discussed in the case is diluted by the technical grounds on which the Safe Harbour was found invalid.

Disappointingly Schrems follows the uncomfortable trend, shown through the PNR saga, of the ECJ withholding fundamental rights analysis in favour of technical, procedural points of law. The implication is that economic and political concerns dominate the strong protection of personal data.

Additionally the authority of the EU is being undermined by the threat of Member State exit and limited protection has been provided by the vague scope of the fundamental rights to privacy and data protection under the Charter.

With mass surveillance ongoing and the emergence of Big Data it is a crucial period for data protection law internationally. I am concerned the direction of surveillance, from targeted to generalised, could be normalised without action. National security legislation can create new norms of acceptable state action with fundamental rights progressively eroded over time. This process, or “ratchet effect,” can repeat as changed norms represent new baselines on which to expand further national security powers. The process can be difficult to counter as politicians are hesitant to repeal national security legislation. The political repercussions if a repeal was followed by an attack could be career ending. However the lack of benefits and

\[\text{\textsuperscript{515}}\text{At 8.}\]
\[\text{\textsuperscript{516}}\text{At 8.}\]
\[\text{\textsuperscript{518}}\text{Ibid.}\]
extensive violation of fundamental rights mean mass surveillance must be challenged. The new standard of adequacy under the Regulation could be a vital participant in this conversation.

With effective implementation and enforcement the Regulation's provisions on algorithmic accountability, data breach reporting and privacy by design and default have substantial promise to improve the standard of adequate protection. I believe a focus on data security, through sector based cyber building codes, will result in higher standards of data protection being promulgated throughout the EU and beyond.

This thesis has canvassed tensions: between an Anglo-American conception of privacy and a European conception of privacy; between the economic interests of data controllers and the privacy of data subjects; between national security and human rights; between innovation nurtured in a protected sphere and innovation from unrestricted processing of personal data. These tensions pull and push and twist the technological path we all walk which is neither fixed nor natural. These issues have bubbled below the public discourse without obvious resolution or widespread contribution.

Speaking to me via private email Max Schrems made a few significant points which are appropriate to share. First, for most people, it may be private actors misusing data which will have the most effect- failing to get a loan due to illegitimate considerations in the algorithmic process for example. However for opposition groups- the media, whistle-blowers, dissenters- as he describes, the “core pillars of our democratic society,” it is the government surveillance which is the bigger problem. However he notes they are not distinct threats but a partnership with previously unknown surveillance powers. For adequacy to have meaning this partnership must be fractured.

Given the lack of resources dedicated to data protection in the EU it is important to consider what key areas should be prioritised- it is unlikely many of my suggestions

---

519 Email from Max Schrems to Henry Flood regarding public and private misuse of personal data (18 January 2017).
will be implemented. In light of this I believe compulsory encryption and compulsory algorithm auditing are vital areas of focus. Encryption would undermine mass surveillance and algorithm auditing could curtail discrimination in automated decisions. They could give meaning to adequacy.

Ultimately adequacy has the potential to redirect the technological path we all walk. It is to this path I want to make my final point.

The National Aeronautics and Space Administration (NASA) recently fast tracked their Wide-Field Infrared Survey Telescope (WFIST) project. The telescope has a field of vision one hundred times that of the Hubble telescope and will assist in measuring the expansion of the universe. The WFIST will also look for planets outside Earth’s solar system and research the nature of dark energy.520

The WFIST was an unexpected donation from the National Reconnaissance Office (NRO), the United States Government Agency in charge of spy satellites.521 The telescope had been conducting surveillance from the skies. The NRO’s new technology has made the WFIST obsolete.

NASA, which struggles for funding yet drives science and innovation on a truly global scale, is using technology hand-me-downs from the United States spying apparatus.

Mass surveillance is a tragic misallocation of our technological resources. Instead of looking out to discover the wonders of the universe we have been spying within.

Privacy is not protected. The economy is not advanced.

This is not adequate. This cannot continue.

521 At 2.
### XI CASES, LEGISLATION AND BIBLIOGRAPHY

**A Table of cases**

**European Union**

<table>
<thead>
<tr>
<th>Case Reference</th>
<th>Case Title</th>
<th>Year</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/73</td>
<td>Nold v Commission of the European Communities</td>
<td>1974</td>
<td>ECR 491</td>
</tr>
<tr>
<td>5/88</td>
<td>Wachauf v Federal Republic of Germany</td>
<td>1989</td>
<td>ECR 2609</td>
</tr>
<tr>
<td>36/75</td>
<td>Roland Rutili v Ministre de l’intérieur</td>
<td>1975</td>
<td>ECR 1219</td>
</tr>
<tr>
<td>C-92/09</td>
<td>Volker und Markus Schecke and Eifert v Land Hessen</td>
<td>2010</td>
<td>ECR I-11063</td>
</tr>
<tr>
<td>C-112/00</td>
<td>Schmidberger v Austria</td>
<td>2003</td>
<td>ECR I-5659</td>
</tr>
<tr>
<td>260/89</td>
<td>Elleniki Radiophonia Tileorasi v Dimotiki Etairia Pliroforissis</td>
<td>1991</td>
<td>ECR 2925</td>
</tr>
<tr>
<td>C-288/12</td>
<td>European Commission v Hungary</td>
<td>2014</td>
<td>CJEU 8 April</td>
</tr>
<tr>
<td>C-291/12</td>
<td>Michael Schwarz v Stadt Bochum</td>
<td>2013</td>
<td>CJEU 17 October</td>
</tr>
<tr>
<td>C-293/12 and C-594/12</td>
<td>Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others</td>
<td>2014</td>
<td>CJEU 8 April</td>
</tr>
<tr>
<td>C-317/04 and C-318/07</td>
<td>European parliament v Council of the European Union and Commission of the European Communities</td>
<td>2006</td>
<td>CJEU 30 May</td>
</tr>
<tr>
<td>C-341/05</td>
<td>Laval un Partneri Ltd v Svenska Byggnadsarbetarförbundet and others</td>
<td>2007</td>
<td>ECR-I 11767</td>
</tr>
<tr>
<td>C-362/14</td>
<td>Schrems v Data Protection Commissioner</td>
<td>2015</td>
<td>CJEU 6 October</td>
</tr>
</tbody>
</table>


Case C-438/05 International Transport Workers’ Federation, Finnish Seamen’s Union v Viking Line ABP, OÜ Viking Line Eesti, [2007] ECR I-10779


European Court of Human Rights


England

Entick v Carrington [1765] EWHC KB J98.

Germany


Ireland


United States


United States v Ivanoc 175 F Supp 2d 36 (D Conn 2001).

B Table of legislation and International Instruments

Europe


Federal Act on Data Protection 1992 (Switzerland).

Federal Data Protection Act 2003 (Germany).


Personal Data Act 1998 (Sweden).


United States

18 USC § 2710.

18 USC § 1030.

Mass Code 201 § 17.04.
Other


C Books


Fred Cate Privacy in the Information Age (Brookings Institute, Washington, 1997).


D Essays and Chapters in Books


E Journal articles


Howard Beales III “Consumer Protection and Behavioural Economics: To be or not to be?” (2008) 4 Competition Policy International 149.


Gloria Fuster “Fighting for your right to what exactly? The convoluted case law of the EU Court of Justice on privacy and/or personal data protection” (2014) Birkbeck Law Review 2(2) 263.


Alison Holman, Dana Garfin and Roxane Silver “Media’s role in broadcasting acute stress following the Boston Marathon bombings” 111 PNAS 93.


Latayna Sweeney “Discrimination in Online Ad Delivery” (2013) 56(5) Communications of the ACM 44.


Janice Tsai and others “The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study” (2010) 22(2) Information Systems Research 254 at 264.


Article 29 Working Party “Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector” (536/14/EN WP 211, Adopted 27 February 2014).


Article 29 Working Party “Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)” (16/EN WP 237, Adopted 13 April 2016).


Internet Resources


Centre for Disease Control “Heart Disease Facts” (August 2015) United States Department of Health and Human Services <www.cdc.gov>.


Kate Lyons and Gordon Darroch “Frexit, Nexit or Oexit? Who will be next to leave the EU” (27 June 2016) The Guardian <www.theguardian.com>.


Kenneth Olmstead and Aaron Smith “Americans and Cybersecurity: Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives” (26 January 2017) Pew Research Centre <www.pewinternet.org>.


H Papers and Reports


Alessandro Acquisti “The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines” (paper presented to OECD Conference Centre, Paris, 1 December 2010).


Ross Anderson and others “Measuring the Cost of Cybercrime” (paper presented at Workshop on the Economics of Information Security, Berlin, June 2012),


Jan Dhont and others “Safe Harbour Decision Implementation Study” (Report for European Commission, Namur, 19 April 2004).


Justus Haucap and Ulrich Heimeshoff “Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization?” (Discussion paper for Düsseldorf Institute for Competition Economics, Düsseldorf, January 2013).


Douwe Korff “Analysis and impact study on the implementation of Directive EC 95/46 in Member States” (Report for European Commission, University of Essex, 2002).

Douwe Korff and Marie Georges “Passenger Name Records, data mining and data protection: the need for strong safeguards” (Report for Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, 15 June 2015).

Mandiant “m-Trends 2015: A View from the Front Lines” (threat report, 2015)


I Other


Email from Max Schrem to Henry Flood regarding public and private misuse of personal data (18 January 2017).

TNS Opinion and Social Special Eurobarometer 423 Cyber Security (Survey for the Directorate-General for Home Affairs, February 2015).

Advocate General Cruz Villalon “Opinion of Advocate General Cruz Villalon on Case C-269/12 Digital Rights Ireland v Minister for Communication, Marine and Natural Resources and Others and Kärntner Landesregierung and Others” (Opinion, ECLI:EU:C:2013:845, Delivered 12 December 2013).