

**CRITICAL ANALYSIS OF VIDEOGAME PRIVACY POLICIES: DATA HANDLING
PRACTICES AND EVALUATING CHILDREN'S DIGITAL PRIVACY RIGHTS IN
EUROPE, U.S., AND CANADA**

Mobeen Imran Shah

LLB(Hons) BVC LLM

A thesis submitted in partial fulfilment of the requirements of
Nottingham Trent University for the degree of
Doctorate of Philosophy

July 2018

Copyright Notice

This work is the intellectual property of the author. You may copy up to 5% of this work for private study, or personal, non-commercial research. Any re-use of the information contained within this document should be fully referenced, quoting the author, title, university, degree level and pagination. Queries or requests for any other use, or if a more substantial copy is required, should be directed in the owner(s) of the Intellectual Property Rights.

ACKNOWLEDGEMENTS

The final outcome of this project required support, guidance and encouragement from many people. First, I must give my sincerest thanks to my lead supervisor, Dr Janice Denoncourt. Janice became director of studies after taking over from Dr Rebecca Wong, who identified my potential and was my initial supervisor. Janice encouraged and supported me every step of the way. She challenged my assumptions and invited me to look at the project from different angles and, therefore, I am highly grateful to her for having played a major part in shaping the project as it is today. I could not imagine doing this without her in my team. Secondly, thanks to Professor Rebecca Parry for her invaluable recommendations. She always made me look at the project with a fresh pair of eyes. She would regularly send me developments relevant to my project, which have further expanded my own knowledge and understanding in the subject area. Thirdly, my sincerest thanks to Dr Ben Oldfield, who provided much-needed support with regard to the choice of videogame websites that were compatible with this study. Fourthly, I thank Dr Colin Wilmott for his valuable insight into data mining techniques. These wonderful people have made this project happen.

I must also thank my family, for their tireless patience, self-sacrifice and encouraging and enduring support, while I was firmly tethered to this mammoth project. I could not have done this without them providing a firm ground that kept me from floating into outer space.

ABSTRACT

The extensive use of the internet by children has given rise to concerns about their digital privacy.¹ The General Data Protection Regulation ('EU GDPR 2018')² treats children as a 'special class of data subjects'³ without clearly explaining how to do so in practice. Privacy policies set out a website's data handling practices, however, they are typically complex, lengthy documents that deter users from reading them.⁴ A comparative analysis examining the adequacy of data privacy laws in the EU, the U.S. and Canada in protecting children's digital privacy is carried out, followed by a multiple-case study evaluation of popular videogame policies. As a result, an original

¹ Cara McGoogan, 'Hackers steal 2.5 million PlayStation and Xbox players' details in major breach' (The Telegraph 1 February 2017) <<https://www.telegraph.co.uk/technology/2017/02/01/hackers-steal-25-millionplaystation-xbox-players-details-major/>> accessed 2 April 2018.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Text with EEA relevance).

³ EU GDPR 2018 Article 8.

⁴ Yannis Bakos, Florencia Marotta-Wurgler, David R. Tossen, 'Does anyone read the fine print? Consumer Attention to standard form contracts' (JSTOR, 2014)

<<https://webcache.googleusercontent.com/search?q=cache:HELW1FvT1j0J:https://www.journals.uchicago.edu/doi/abs/10.1086/674424+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 April 2018.

child-friendly model privacy policy was drafted, designed to inform the development of best practice in treating children as a special class of data subjects.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	II
ABSTRACT	III
TABLE OF LEGISLATION	X
TABLE OF CASES	XVI
TABLE OF ABBREVIATIONS	XX
LIST OF TABLES.....	XXI
LIST OF FIGURES	XXIII
GLOSSARY	XXIV
TABLE OF CONTENTS	V
CHAPTER ONE: INTRODUCTION TO CHILDREN’S DIGITAL PRIVACY RIGHTS IN VIDEOGAME WEBSITES	2
1.1 INTRODUCTION.....	2
1.2. BACKGROUND TO THE PROBLEM.....	13
1.3. LITERATURE	25
1.4. SIGNIFICANCE OF THE STUDY	30
1.5. PRIMARY RESEARCH QUESTIONS	32
1.6. RESEARCH METHODOLOGY	33
1.7. OVERVIEW AND STRUCTURE OF THE THESIS	46

CHAPTER TWO: UNDERSTANDING THE CONCEPTS OF PRIVACY AND DATA PROTECTION 49

2.1. INTRODUCTION49

2.2. DEFINITION OF PRIVACY..... 50

2.3. RIGHTS OF CHILDREN IN THE EU 55

2.4. IMPORTANCE OF PRIVACY IN THE CYBER WORLD 57

2.5. DIGITAL PRIVACY AWARENESS OF PARENTS AND CHILDREN62

2.6. DATA PROTECTION AND PRIVACY CODIFIED IN LEGISLATIVE INSTRUMENTS72

2.7. DATA PROTECTION AND RIGHT TO PRIVACY – TWO OVERLAPPING OR SEPARATE RIGHTS75

2.8. CONCLUSIONS78

CHAPTER THREE: EUROPEAN DIGITAL PRIVACY LEGISLATION80

3.1. INTRODUCTION80

3.2. DATA PROTECTION DIRECTIVE 95/46/EC – NOW REPEALED.....85

3.3. E-PRIVACY DIRECTIVE (THE EU COOKIE DIRECTIVE)112

3.4. CONCLUSIONS118

CHAPTER FOUR: DATA PROTECTION AND PRIVACY FRAMEWORK IN THE U.S. AND CANADA 121

4.1. INTRODUCTION121

4.2. COMPARATIVE LAW METHODOLOGY 121

4.3. REGULATION OF DATA PROTECTION IN THE U.S. 123

4.4. CALIFORNIA’S ONLINE PRIVACY PROTECTION ACT 2003	134
4.5. DELAWARE’S ONLINE PRIVACY PROTECTION ACT	136
4.6. WASHINGTON STATE PRIVACY LAWS	137
4.7. FINDINGS FROM THE U.S. BASED DATA PRIVACY LAWS	138
4.8. GLOBAL INFORMATION GUIDELINES: FAIR TRADE PRACTICES	141
4.9. CANADA’S PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENT ACT 2000	142
4.10. FINDINGS	145
4.11. THE BIG PICTURE: CONCLUSIONS	155
CHAPTER FIVE: PART 1 – ONLINE GAMES CASE STUDIES: PRIVACY POLICIES AND CHILDREN	158
5.1. INTRODUCTION	158
5.2. CHILDREN’S DIGITAL PRIVACY	159
5.3. MULTIPLE CASE STUDY METHODOLOGY	160
5.4. CRITERIA FOR EVALUATING THE PRIVACY POLICIES OF VIDEOGAME CASE STUDIES.....	167
5.5. EVALUATION OF THE PRIVACY POLICIES OF 10 VIDEOGAME WEBSITES SELECTED FOR THIS THESIS	174
5.6. COMPARATIVE PRIVACY POLICY CONTENT ANALYSIS	212
5.7. THE REGISTRATION PROCEDURE IN VIDEOGAME WEBSITES	213
5.8. CONCLUSION AND RECOMMENDATIONS REGARDING PRIVACY POLICIES FOR CHILDREN	215

CHAPTER SIX: PART 2 – ONLINE GAMES CASE STUDIES: PRIVACY POLICIES AND GOVERNING DATA PRIVACY LAW 219

6.1. INTRODUCTION219

6.2. OVERVIEW OF THE KEY LEGISLATION IN THE U.S. AND EU FOR EVALUATING PRIVACY POLICIES220

6.3. OVERVIEW OF FINDINGS OF THE STUDY OF PRIVACY POLICIES OF ONLINE VIDEOGAME WEBSITES GOVERNED BY U.S. DATA PRIVACY LAW 240

6.4. VIDEOGAME WEBSITES GOVERNED BY EUROPEAN DATA PRIVACY LAW 242

6.5. LEGAL ANALYSIS OF THE STUDY OF PRIVACY POLICIES OF THE VIDEOGAME WEBSITES GOVERNED BY EU DATA PRIVACY LAWS 257

6.6. CONCLUSIONS AND RECOMMENDATIONS258

CHAPTER SEVEN: ORIGINAL CHILD-FRIENDLY MODEL PRIVACY POLICY 266

7.1. INTRODUCTION266

7.2. STUDY OF PRIVACY POLICIES AS BENCHMARKS TO GUIDE THE ORIGINAL CHILD-FRIENDLY MODEL PRIVACY POLICY 268

7.3. OVERVIEW OF DISNEY.COM PRIVACY POLICY.....269

7.4. OVERVIEW OF THE BBC.CO.UK/CBEEBIES PRIVACY POLICY 273

7.5. OVERVIEW OF THE HARRY POTTER WEBSITE ([WWW.WARNERBROS.CO.UK](http://www.warnerbros.co.uk)) PRIVACY POLICY.....274

7.6. BEST PRACTICES OBTAINED FROM THE STUDY OF THE DBH PRIVACY POLICIES275

7.7. ORIGINAL CHILD-FRIENDLY MODEL PRIVACY POLICY 281

7.8. CHANGES PROPOSED IN THE CHILD-FRIENDLY MODEL PRIVACY POLICY..... 284
7.9. RECOMMENDATIONS AND CONCLUSIONS288

CHAPTER EIGHT: CONCLUSION291

8.1. INTRODUCTION291
8.2. KEY ISSUES OF THE RESEARCH293
8.3. COMPARATIVE FINDINGS BETWEEN LEGISLATION IN
THE EU, THE U.S. AND CANADA300
8.4. FINDINGS OF THE VIDEOGAME MULTIPLE CASE STUDY302
8.5 BEST PRACTICES: MINI-CASE STUDY.....309
8.6. ORIGINAL CHILD-FRIENDLY MODEL PRIVACY POLICY309
8.7. LIMITATIONS OF THE STUDY312
8.8. RECOMMENDATIONS FOR FUTURE RESEARCH315
8.9. THE FINAL MESSAGE316
ANNEX 1 – CHILDREN’S ONLINE PRIVACY PROTECTION ACT 322
ANNEX 2 – TEXT OF EU GENERAL DATA PROTECTION REGULATION 2018
ARTICLES 5, 6, 7, 12, 13 & 15.....324

BIBLIOGRAPHY

TABLE OF LEGISLATION

Australia

Privacy Act 1988 Act No. 119 of 1988

Austria

Datenschutzgesetz 2000 (DSG 2000), Austrian Federal Law Gazette part I No.
165/1999

Canada

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982

Digital Privacy Act (S.C. 2015, c. 32)

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5 Privacy

Act of 1983

China

Cybersecurity Law of the People's Republic of China

Council of Europe

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, ETS 108, 1981

European Convention on Human Rights 1950

European Union

Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004)

Charter of Fundamental Rights of the European Union 2000

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection law

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations

Directive 98/48/EC of the European Parliament and of the European Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations

Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2012

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Text with EEA relevance)

Treaty on European Union 1992

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

India

Information Technology Act 2000 (No. 21 of 2000)

International Law

International Covenant on Civil and Political Rights 1966

UN General Assembly, Convention on the Rights of the Child, 20 November
1989, United Nations, Treaty Series, vol. 1577, p. 3

United Nations Convention on the Rights of Child 1990

Universal Declaration of Human Rights 1948

Italy

Italian Personal Data Protection Code Legislative Decree no. 196 of 30 June 2003

Hungary

Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on
Freedom of Information

Netherlands

Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens
(Wet bescherming persoonsgegevens)

Spain

Kingdom of Spain, Royal Decree 1720/2007 of 21 December approving the Regulations
implementing Law 15/1999 on the Protection of Personal Data 2007

United Kingdom

Children Act 2004 Chapter 31

Data Protection Act 1998

The Motor Vehicles (Driving Licences) Regulations 1999

Data Protection Act 2018

Sexual Offences (Amendment) Act 2000

European Union (Withdrawal) Bill 2017–19

Family Law Reform Act 1969 (England and Wales)

Mental Capacity Act 2005

Minors' Contract Act 1987

United States

U.S. Federal Laws

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505

Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970)

Federal Trade Commission Act of 1914 15 U.S.C. ss. 41–58

Presidential Recordings and Materials Preservation Act of 1974

U.S. State Laws

California

California Financial Information Privacy Act (Financial Code § 4053(d))

California Online Privacy Protection Act 2003 (California Business & Professions Code sections 22575-22579)

Delaware

Delaware Online Privacy Protection Act

Washington

Revised Code of Washington

TABLE OF CASES

European Union

European Court of Human Rights

Gaskin v United Kingdom (1989) 12 EHRR 36

Campbell v UK A 233 (1992) 15 EHRR 137

Goodwin v United Kingdom, no. 28957/95, 11 July 2002

Grand Chamber Case of Delfi AS v Estonia (Application no. 64569/09) 16 June 2015

Handyside v the United Kingdom (5493/72) [1976] ECHR 5

European Court of Justice

Case C-524/06 *Heinz Huber v Bundesrepublik Deutschland* [2008]

Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España*

SAU [2008]

Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*

GmbH v Tele2 Telecommunication GmbH [2009]

C-92/09 and C-93/09 *Markus Schecke and Hartmut Eifert* [2010] ECR I -11063

Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et*

éditeurs SCRL (SABAM) [2011]

Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en*

Asiel and Minister voor Immigratie, Integratie en Asiel v M and S 12 December 2013

Case 131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de*

Datos, Mario Costeja González C - [2014]

(C-362/14) *Maximillian Schrems v Data Protection Commissioner* 6 October 2015

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary (Application no.

22947/13) 2 February 2016

Case C-582/14 and Case C-362/14 *Patrick Breyer v Bundesrepublik Deutschland* 19

October 2016

Germany

Germany, Case No. 11 LC 114/13

United Kingdom

Applause Store Productions Ltd & Firshet v Raphael [2008] EWHC 1781 (QB)

Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74, CA
De Francesco v Barnum (1890) 45 Ch D 43

Durant v Financial Services Authority [2003] EWCA Civ 1746, CA

Fawcett v Smethurst (1914) 84 LKB 473

Gillick v West Norfolk & Wisbech Area Health Authority [1986] AC 112 House of
Lords

Nash v Inman [1908] 2 KB 1, CA

United States

U.S. Federal Case Law

Boyd v United States, 116 U.S. 616 (1886)

Griswold v Connecticut, 381 U.S. 479 (1965)

Laird v Tatum, 408 U.S. 1 (1972)

McElrath v Califano, 615 F.2d 570 (3d Cir. 1980)

Meyer v Nebraska, 262 U.S. 390 (1923)

Nixon v Administrators of General Services, 433 U.S. 425 (1977)

Paul v Davies, 424 U.S. 693 (1976)

Pierce v Society of Sisters, 268 U.S. 510 (1925)

Planned Parenthood v Danforth, 428 US 52 (1976)

Roe v Wade, 410 U.S. 113 (1973)

St Michael's Convalescent Hospital v California, 643 F.2d 1369 (9th Cir. 1981)

Whalen v Roe, 429 U.S 589 (1977)

U.S. State Case Law

District of Arizona

FTC v LabMD No. 1:12-cv-3005 (N.D. Ga. Nov. 26, 2012)

District of Montana

Mortensen v Bresnan Communications CV 10-13-BLG-RFC. (D.Mont. Nov. 15, 2010)

State of California

The people of the State of California v Kaiser Foundation Health Plan Inc. Case number

RG14711370 [2014]

TABLE OF ABBREVIATIONS

General

California Online Privacy Protection Act	CalOPPA
Charter of Fundamental Rights of the European Union 2000	EUCFR
Children’s Online Privacy Protection Act 1998	COPPA
Delaware Online Privacy Protection Act	DOPPA
European Convention on Human Rights	ECHR
European Court of Human Rights	ECtHR
European Court of Justice	ECJ
European Data Protection Supervisor	EDPS
European Union	EU
Federal Trade Commission	FTC
Personal Information Electronic and Documents Act	PIPEDA
United Kingdom	UK
United Nations Convention on the Rights of Child	UNCRC
United States	U.S.
Universal Declaration of Human Rights 1948	UDHR
Information Commissioner’s Office	ICO

LIST OF TABLES

<i>TABLES</i>	<i>PAGE</i>
Table 1 Codification of privacy law in the pre-digital environment	53
Table 2 - Chronology of global data protection law	72
Table 3 - Online game website ranking/percentage and source (2015)	166
Table 4 – List of criteria for studying privacy policies	168
Table 5 Videogames selected for the multiple case study; their publishers and location of headquarters	169
Table 6 Criterion 1 - Location of privacy policy	175
Table 7 Criterion 2 - Length and wording of the privacy policy	176
Table 8 Criterion 3 - Governing legislation	184
Table 9 Criterion 4 – Privacy rules involving the Privacy Shield Framework to safeguard transfer of data between the EU and the U. S	186
Table 10 Criterion 5 - TRUSTe Privacy Certification	188
Table 11 Criterion 6 – Collection of Information from children	190
Table 12 Criterion 7 - Third parties collecting personal information	197
Table 13 Criterion 8 – Cookies and other tracking technologies	200
Table 14 Criterion 9 – Methods to disable cookies and other third-party tracking technologies.....	203
Table 15 Criterion 10 – Parental consent mechanism	207
Table 16 Criterion 11 – Players’ right to Subject Access Requests (SAR)	211

Table 17 Criterion 1 – Location of privacy policy	221
Table 18 Criterion 2 – Length and wording of the privacy policy	222
Table 19 Criterion 3 – Governing legislation	224
Table 20 Criterion 4 - Privacy rules involving Privacy Shield Framework to safeguard transfer of data between the EU and the U. S	227
Table 21 Criterion 5 – TRUSTe Privacy Certification	228
Table 22 Criterion 6 – Collection of information from children	230
Table 23 Criterion 7 –Third parties collecting personal information	231
Table 24 Criterion 8 - Cookies and third-party tracking technology and Criterion 9 - Methods to disable cookies and other third-party tracking technologies	233
Table 25 Criterion 10 – Parental consent mechanism	236
Table 26 Criterion 11 – Players’ right to subject access request	239
Table 27 Criteria 1 – Location of privacy policy and Criterion 2 – Length and wording of privacy policy	242
Table 28 Criterion 3 – Governing legislation	244
Table 29 Criterion 6 – Collection of information from children	245
Table 30 Criterion 7 – Third parties collecting personal information	248
Table 31 Criterion 8 - Cookies and other tracking technologies	249
Table 32 Criterion 9 – Methods to disable cookies and third-party tracking technologies	253
Table 33 Criterion 10 - Parental consent mechanism	254
Table 34 Criterion 11 – Players’ right to subject access requests	256

LIST OF FIGURES

<i>FIGURES</i>	<i>PAGE</i>
Figure 1 Privacy of personal information ranks third in order of importance.....	64
Figure 2 Lack of awareness regarding the types of data collection	65
Figure 3 Usage factors parents will take into consideration to protect children’s digital privacy	66
Figure 4 Privacy policy awareness of children aged 9-11 and 14-19-years-old	68
Figure 5 Reasons for not reading privacy policies	69

GLOSSARY

A

Access time

The time taken to locate and retrieve stored information in a computer

Ad network providers

Brokers who gather unsold inventory from publishers and sell it to advertisers

Ad serving technologies

Technology that allows placing advertisements on websites

Advertising conversion rates

The total number of visitors that carry out a particular task such as membership registration

Age gating mechanism

An age verification process that allows or denies access to age-restricted resources

Analytic provider

A business that carries out data analytics to explore and gain insight into businesses' data

Analytic technologies

Hardware and software solutions businesses use to carry out statistical analysis of data to uncover interesting patterns and useful knowledge to improve business practices

Anonymous data/ Anonymised data

Data from which it is not possible to identify individuals, so they remain anonymous

Authentication data

Data which confirms the identity of a person or object while using identity documents or verifying the authenticity of a website

Automated message

A voice or text message recording delivered to multiple devices automatically

Avatar

An image representing a player in a videogame

B

Behavioural targeted advertising

Online adverts targeted towards consumers based on the web pages they visit, their interaction with the website, their preference and their use of the services

Beta tester position

The last stage of testing carried out on videogame software before its commercial release

Browser settings

User preferences which control web tracking mechanisms such as cookies

Browser type

Software application allowing access to the internet on a computer

Browser web storage

Storage of vast quantities of data on the user's browser without affecting the website's performance

Business Intelligence Company

A company which can provide an analysis of an organisation's data for corporate decision makers to improve efficient working of the business and gain a competitive advantage over rivals

C

Chat Bot

A computer programme designed to simulate conversation in human interaction.

Clear gifs (graphics interchange format)

Information gathering that helps websites to learn about the visitor's use of the service and target ads accordingly

Cloud service

Services such as data storage and back-up solutions by a cloud service provider

Cookies/HTTP (Hypertext transfer protocol) cookies

A small text file generated when a person visits a website, which stores information about the user

Copyright

The exclusive right to reproduce and distribute creative work

Cross-apps advertising

The collection of data across various applications to deliver targeted advertising based on consumer preferences

Cross-device tracking tools

Programmes enabling the monitoring of users across multiple devices so that advertisements can be targeted by brands towards that user

Cyber trolling

The posting of upsetting and hurtful information in an online community that is intended to invoke an emotional response

D

Data analytics

Data analysis exploring interesting patterns that help businesses gain useful insight

Data portability

Transfer of data subject's personal information between different devices

Database

A means of storing large quantities of data into a computer in such a way that it can easily be accessed and altered

Depersonalisation of data

The process of making data anonymous so that it cannot be used to identify an individual

Device fingerprints

The use of fingerprints to identify an individual and restrict access to a device to that individual

Device identifier

A unique number that is associated with a particular device such as a smartphone

Digital certificate

Means enabling the secure exchange of information over the internet using public key instructors.

Dynamic IP address (Internet Protocol Address)

Code assigned to a network to recognise the device that change over time

E

Encryption

The conversion of data into a secret code to prevent unauthorised access

F

Facsimile

A copy of written material

File sharing service

A serving enabling the accessing and storing of information in the cloud

First-party cookies

Cookies that are created and stored on a user's computer when a user visits a website

FTP (File Transfer Protocol)

The transfer of computer files between a service provider and service requester

G

Game metrics

Information stored in various formats, which can be transformed to become interpretable

Google Analytics

A service which can track the number of visitors and their behaviour on a website *Gross domestic product (GDP)*

The monetary value of the total number of goods and services produced in a country

H

HTML 5 (Hypertext Markup Language) cookies

The provision of a cookie like storage option available in HTML 5

Hypertext Markup Language (HTML)

A collection of symbols and codes that are inserted into a file for displaying on an internet browser page

I

In-game interactions

Interaction forms available within a game such as chat rooms

International mobile equipment identity (IMEI)

A 15 or 17 digit code that identifies mobile phone sets

IP address (internet protocol address)

A number assigned to a device that is paired to a network so that other devices can identify it

M

Media access control (MAC)

Unique identification and access control given to each piece of hardware

Media audience research firm

A firm that carries out research to understand the media market, analyses data sets, studies audience reaction and targets the audience of the media

Mobile analytics

Analyses of data created on mobile platforms such as mobile applications to improve use of service

Monetisation rate

The rate at which an object is accepted as a medium of exchange

N

National identification number

Information used by governments to identify and track their citizens for multiple reasons

O

Ombudsman

A person appointed to resolve disputes between parties

Online identifier

A name which associates natural persons with their devices, such as an email address

Operating system version

Software that controls the operations of a computer including managing tasks and executing programs

P

Persistent identifier

Identifies a specific file or digital object

Petabytes of data

A unit of measurement of the memory or data storage capacity

Phishing attack

The attempt to acquire sensitive personal information for malicious purposes

Pixel tag

Collects information from visitors and their use of the web service, sent back to the respective platform for marketing purposes

Pop ups

Small windows that suddenly pop on the screen and contain advertisements

Product keys

Confirm the originality of the software program copy

Profiling

Records every action undertaken by consumers online

Public key technology

Converts digital information into an unreadable format

Q

Quantitative data

Studies the quantification or measuring of data with numbers

R

Random access memory (RAM)

Temporarily stores data on a computer's processor

Recitals

Present the reasons behind the promulgation of the piece of legislation

Record keeping systems

Records of an organisation that are created maintained and/or disposed of

S

Scripts

Computer language containing a series of commands performed by another program rather than the computer's processor

Silverlight application storage

Provides users with additional storage space on their computer

Small and medium enterprises

Employ fewer than 250 people with an annual turnover not exceeding 50 million euros⁵

Statistical software programme

Carries out statistical and data analysis on financial and marketing applications

Subsidiary company

Owned and controlled by another company

T

Temporary files

Store information temporarily when a program lacks sufficient memory space

Third-party ad server

⁵ http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en accessed 12 April 2017

Independent companies that deliver targeted ads to consumers based on their preferences

Third-party tracking technology

An external tracking application that tracks consumer behaviour, assesses the effectiveness of advertising and shares the information with its partners

Time stamps

Reveal the exact time and date at which the event occurred through a digital recording

Tracking pixels

A graphic with dimensions 1x1 pixel loaded when a user visits a website

U

Uniform resource locator (URL)

Also known as a web address, is clicked on to access a particular web page

Unique identifier

Unique to a particular object for identification and contact purposes

V

Virtual items

Intangible goods that can be used online such as in videogames and purchased with money

W

Web analytic tools

Analyse the behaviour of users interacting with the website. The application helps companies understand web usage and the effectiveness of advertising campaign

Web beacon

An invisible graphic image that is only 1x1 pixel and collects information about the way the user interacts with the website

Website privacy settings panel

Specifies the privacy settings for a website

CHAPTER ONE

INTRODUCTION TO CHILDREN'S DIGITAL PRIVACY RIGHTS IN VIDEOGAME WEBSITES

1.1. Introduction

*'... a balance between empowerment and protection of children in the online world has to be found.'*¹

This thesis represents an effort to evaluate how best a balance can be achieved in respect of the empowerment of children and their protection in the online world. Ideally children should be in control of their own data, since arguments exist for children's empowerment drawing on 'new sociology of childhood' where children are theorised as competent social actors.² Studies suggest that children may lack formal legal capacity but their understanding of law in everyday life, as well as their contribution towards empirical studies demonstrate that they possess legal capability.³ Owing to this competence, there are calls to involve children's opinion and experiences in services that are provided for their benefit.⁴ However the online environment presents particular challenges that are largely under-addressed in existing literature.

¹ Final recommendations made after a 12-day discussion to foster deeper understanding of the effects of children's engagement with social media and information and communications technologies (ICT) Committee on the Rights of the Child report of the 2014 day of general discussion 'Digital media and children's rights' (UN Committee on the Rights of Child September 2014) <http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf> accessed 4 March 2018.

² Dawn Watkins and others, Exploring Children's Understanding of Law in Their Everyday Lives; 'Assessing Children's Understanding of Law through Digital Gaming' (2018) 38(1) Legal Studies

³ Ibid.

⁴ Ashford, A, 'Involving children in decision making' (Commissioner for Children Tasmania) <<https://www.childcomm.tas.gov.au/wp-content/uploads/2015/06/Guide-to-making-decisions-booklet.pdf>> accessed 1 December 2018.

In the digital world, as technology rapidly grows, children have become one of the largest demographic online user community. Increasing numbers of younger children are interacting with the online community that has led to escalating concerns of safety and child protection online.⁵ Among these are concerns regarding the collection of data. There are arguments that children should be empowered to protect themselves against online dangers; to be aware of their responsibilities so as to effectively safeguard their interests online.⁶ Texts adopted by the Council of Europe and other international organisations emphasise the need for children's empowerment through education which includes digital literacy so that children can identify and understand harmful content.⁷ A child-friendly data policy is an important way in which this empowerment can be achieved and is explored in depth in this thesis. The recently introduced EU GDPR⁸ treats children as a special class, recognising that children are vulnerable and therefore need additional protection online (see section 1.1.1.) The discussion regarding children's vulnerability and empowerment is carried out in the following sections.

An example which illustrates the potential risks to children in the online world is the Minecraft security breach. When independent security expert Troy Hunt received information that stolen data was circulating on dark sites, he found that the data of

⁵ Brian O' Neill, 'Internet Policies: Online Child Protection and Empowerment in a Global Context' (London: Routledge 2013)

⁶ Council of Europe, 'Protecting children's rights in the digital world: an ever-growing challenge' (Europa) <<https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1?desktop=true>> accessed 23 November 2018.

⁷ Ibid.

⁸ Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016

more than seven million Minecraft⁹ members had been accessed by hackers.¹⁰ Worryingly, although the data had been accessed in February 2016, the breach was only discovered months later. Minecraft is a sandbox videogame¹¹ extremely popular amongst children. Some of the risks related to unlawfully accessed data can include identity theft, and disclosure to third parties. Data privacy¹² concerns regarding children are part of the wider context of data protection and privacy issues.

As a major online user community, children may be vulnerable to numerous online risks, including grooming, abuse and commercial exploitation, while performing online activities. One of the concerns regarding children in the online community is the age at which they can appropriately agree to submit personal information. There is a lack of international consensus as to the age at which children can give consent, partly due to cultural variations across the EU and beyond (*see 4.10.1*) Different data privacy jurisdictions apply inconsistent ages at which children can provide online consent (*see 1.2.3*). This is troublesome because nation states offer varying levels of data protection, and children in one country playing a videogame registered in a different country would not know if they will be treated as a child or an adult for the purposes of data processing¹³ (*see 4.10.1*).

⁹ Minecraft is a videogame created and designed by Swedish game designer Markus 'Notch' Persson and later fully developed and published by Mojang. It is a game about placing blocks and going on adventures <<https://minecraft.net/>> accessed 3 December 2017.

¹⁰ 'Hackers steal millions of Minecraft passwords' (*BBC News*, 29 April 2016)

<<http://www.bbc.co.uk/news/technology-36168860>> accessed 27 October 2017.

¹¹ A sandbox is a style of game in which minimal character limitations are placed on the gamer, allowing the gamer to roam and change a virtual world at will <<https://www.techopedia.com/definition/3952/sandbox-gaming>> accessed 3 December 2017.

¹² In this thesis, the terms 'data privacy', 'online privacy' and 'digital privacy' will have the same meaning; the right of an individual to maintain personal information privacy on the Internet.

¹³ Mary Madden and others, 'Teens, social media and privacy' (Pew Research Center, 21 May 2017)

<<http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>> accessed 3 December 2017.

This is a problem because technology appears to be developing at a greater rate than the information, awareness and skill required to keep up with it. For instance, some online users experience difficulty in operating their privacy settings through their respective browsers.

Given the variety of options and the risks associated with the online world, this thesis captures the widest range for childhood and considers the age of 18 years as an upper limit for providing online consent, as discussed in detail at pages 17 - 22. Protecting children in the digital environment is vital because developmental psychology proves 'adolescents' can be more active and risk-prone online.¹⁴ Children may not have the mental maturity to exercise caution while online. Children may be vulnerable (see section 1.1.1.)¹⁵, they may easily divulge personal information about themselves and others (parents/legal guardians) and become exposed to online threats.

The consequences of dataveillance¹⁶ practices have led to children being treated as 'algorithmic assemblages ... with the possibility that their complexities, potentialities and opportunities may be circumscribed'.¹⁷ Multiple studies suggest that children are spending longer hours online, averaging 15 hours a week for youngsters aged five to 15 years.¹⁸ The Pew Internet & American Life Project undertook a survey of children aged 12 to 17 years and found that 97% played online videogames.¹⁹ The EU Kids Online²⁰ survey of the activities carried out by online users revealed that, in the UK,

¹⁴ Andrew Hope, 'Risk-Taking, Boundary-Performance and Intentional School Internet "Misuse"' (2007) 28(1) *Discourse: Studies in the Cultural Politics of Education* 87.

¹⁵ EU GDPR Recitals 35 and 78

¹⁶ Oxford Dictionary <<https://en.oxforddictionaries.com/definition/dataveillance>> accessed 13 April 2018. The practice of monitoring digital data relating to personal details or online activities.

¹⁷ Deborah Lupton and Ben Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) 19(5) *New Media & Society* 780.

¹⁸ 'Children and Parents: Media Use and Attitudes Report 2016' (Ofcom, 2016)

<<https://www.ofcom.org.uk/research-and-data/media-literacy-research/children/children-parents-nov16>> accessed 24 December 2016. Some children spend up to 7.5 hours in front of a screen: Kim Bartel Sheehan, *Controversies in Contemporary Advertising* (SAGE 2014).

¹⁹ Amanda Lenhart and others, 'Teens, Videogames and Civics' (Pew Research Centre, 16 September 2008) <<http://www.pewinternet.org/2008/09/16/teens-video-games-and-civics/>> accessed 27 October 2017.

²⁰ EU Kids Online is a multinational research network. It seeks to enhance knowledge of European children's online opportunities, risks and safety. EU kids online (LSE 2016).

<<http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>> accessed 7 February 2018.

83% of children between the ages of nine and 16 play online games; whereas 92% use the internet for schoolwork.²¹

The online gaming industry is now bigger than the Hollywood film industry.²² Children are playing longer hours on the internet. Tamara Gaffney, principal analyst at ADI (Adobe Digital Index),²³ compared the revenue of box-office movies on their opening days with the revenue of top videogames on their opening days.²⁴ According to the report, sales of the game Metal Gear Solid V: The Phantom Pain were US \$179 million on its first day; whereas, in comparison, the movie 'Harry Potter and the Deathly Hallows Part 2' brought in US \$91 million with a much bigger budget.²⁵

The internet is available on multiple platforms, attracting millions of users, including children. Such an open and easily accessible online world can be fraught with potential safety and privacy issues. Massive profiling creates an obligation to safeguard the right to privacy and disclosure to unauthorised individuals.²⁶ Children are particularly vulnerable as they may not be risk-averse to digital privacy threats

²¹ Sonia Livingstone and others, 'Risks and Safety for Children on the Internet: The UK Report' (The London School of Economics and Political Science December 2010).

<[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/National%20reports/UKReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf)> accessed 17 November 2017.

²² 'The Biggest Entertainment Markets in the World' (Business Tech, 31 May 2015)

<<https://webcache.googleusercontent.com/search?q=cache:iq33Zf5jsQUJ:https://businesstech.co.za/news/lifestyle/88472/the-biggest-entertainment-markets-in-the-world/+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 27 October 2017. Christina Holtz-Bacha and Marion R. Just, *Routledge Handbook of Political Advertising* (Routledge 2017). Videogames generate greater revenue than the movie and music industry.

²³ Adobe Digital Index publishes research on digital marketing and other topics of interest to senior marketing and e-commerce executives across industries ADI holiday 2015 report

<<https://webcache.googleusercontent.com/search?q=cache:Hw5r6isDf2cJ:https://landing.adobe.com/en/na/solutions/digital-index/246230-2015-holiday-shopping-infographic/index.html+&cd=2&hl=en&ct=clnk&gl=uk>> accessed 7 February 2018.

²⁴ 'U.S. Gaming Trends Report' (Adobe. 12 October 2015) <<https://www.slideshare.net/adobe/us-gaming-trends-report/1>> accessed 7 February 2018.

²⁵ Ibid.

²⁶ John Wang, *Data Mining: Opportunities and Challenges* (IGI Global 2003).

through the accumulation of personal information by surreptitious mechanisms.²⁷

They may not exhibit the same attitudes towards privacy that adults do.

When children play videogames, they submit personal information to register with the website, take part in surveys, chat, social forums etc (see 5.7). It is necessary to consider if children's digital privacy is adequately protected from the perspective of data analysis techniques and data privacy regulation. A comparative legal analysis between the data privacy regimes of predominantly English-speaking legislatures, namely the U.S. and Canada, will be carried out (*Chapter 4*). Additionally, the data privacy laws of the European Union, which is an important contributor to the world gaming market, will also be studied (*Chapter 3*). The analysis will highlight strengths and weaknesses between the selected legislatures, laws and implementation.

This can help devise solutions for the legal protection of children's digital privacy rights from excessive commercial exploitation by means of data collection practices, including cookies,²⁸ web beacons,²⁹ scripts³⁰ and ad analytics.³¹

This study carries out a comparative legal analysis of data protection and privacy law in 3 legislatures from a perspective of the safeguarding of children online. The law is moving fast and regulated subject to amendments considering modern technology

²⁷ Stephanie Simon, 'Data Mining Your Children' (Politico, 2014) <http://www.politico.com/story/2014/05/data-mining-your-children-106676_Page2.html> accessed 24 December 2016.

²⁸ Cookies are small text files that are downloaded onto a user's computer or smartphone when they visit a website. It helps to remember user's devices as well as store information about their preferences or past actions. 'Cookies and Similar Technology' (ICO) <<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>> accessed 18 March 2017.

²⁹ Web beacons, pixel tags or clear gifs are single-pixel graphics interchange format (GIF) that are bits of programming code included in web pages, emails and ads that notify the website when those web pages, emails or ads have been viewed or clicked on. 'Use of Cookies and Similar Technology' (Adobe, 16 June 2016) <<http://www.adobe.com/uk/privacy/cookies.html>> accessed 18 March 2017.

³⁰ Scripts are also embedded within the website to measure how it is used and which links are clicked: Ibid.

³¹ Ad analytics use website analytic tools such as ad servers to quantify the effectiveness of digital advertising Wes Nichols, 'Advertising Analytics 2.0' (*Harvard Business Review*, March 2013) <<https://hbr.org/2013/03/advertising-analytics-20>> accessed 18 March 2017.

such as social media, cookies and similar technology;³² which introduce sophisticated methods of tracking digital personal data.

1.1.1. The EU General Data Protection Regulation and Children as a Special Class

With new challenges to digital privacy, legislation arguably ought to evolve with needs of society, especially children, who are a key user group of the internet. This along with the EU GDPR's acknowledgement in Recitals 38 and 75 that children are vulnerable establishes the argument that children need special protection. The earlier EU Data Protection Directive 95/46/EC³³ did not provide rules on protecting children's digital privacy.

The new EU GDPR 2018³⁴ introduced by the European Commission aimed to do just that.³⁵ The new EU GDPR 2018 will overhaul the data privacy regime in the EU. It will have consequences for U.S. and Canada based organisations that collect and process data belonging to European citizens. It provided special rules for protecting children's digital privacy. Children under 16 years will require lawful consent from the holder of parental responsibility,³⁶ but member states are authorised to reduce this age to 13 years. This is an issue because varying ages for consent can lead to uncertainty as to whether a person is treated as a child or adult across legislatures (*see 4.10.1*). As

³² Richard Beaumont, 'The GDPR, Cookie Consent and Customer Centric Privacy' (Optanon by one trust, 13 May 2016)

<https://www.cookie-law.org/blog/2016/5/13/the-gdpr,-cookie-consent-and-customer-centric-privacy/> accessed 21 February 2018.

³³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³⁴ Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016

³⁵ Provisions of EU GDPR 2018, that are relevant to this thesis are attached as Annex 2 at the end of this document.

³⁶ EU GDPR 2018 Article 8 (1).

European member states adopted the EU GDPR 2018 on 25th May 2018,³⁷ it should be determined if the new regulations have struck the right balance between protecting citizens' digital privacy rights and the overwhelming burdens imposed on the competitiveness of business organisations. This thesis addresses the need for additional protection of children as a special class of data subjects. The term 'special class of data subjects' is self-invented for the purposes of clarity of discussion and refers to the notion that some children may not have the requisite capacity to remain risk averse online. They may easily divulge information about themselves and third parties as well. The earlier Directive 95/46/EC treated both adults and children alike under the umbrella term 'data subjects.' It applied to people generally rather than to making any special cases for any categories of persons such as children specifically. The EU GDPR recognised that children 'merit special protection'³⁸, that they may be less aware of risks. Therefore, they need special protection with respect to the collection of personal data. The EU GDPR has provided specific rules that expressly deal with the protections given to children when processing their personal data³⁹ such as separate provisions applicable to children's consent;⁴⁰ that processing based on legitimate interests is overridden when data subject is a child⁴¹; and information is to be presented in a transparent, concise and plain language when data subject is a child.⁴² The EU GDPR also refers to children as vulnerable natural persons in Recital 75 that may be exposed to risks of varying severity potentially leading to harm where

³⁷ 'Guidance: What to Expect and When (ICO) <<https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/guidance-what-to-expect-and-when/>> accessed 3 December 2017.

³⁸ EU GDPR Recital 38.

³⁹ EU GDPR Recital 71 – children's personal data should not be subject to profiling.

⁴⁰ EU GDPR Article 8.

⁴¹ EU GDPR Article 6(1).

⁴² EU GDPR Recital 58 and Article 12(1).

personal data processing can reveal sensitive information. UNICEF established guidelines for companies processing personal data of children under 18 years of age, warranting specific protection when processing their data.⁴³ Maintaining the theme of special provisions, this thesis refers to children as a ‘special class of data subjects’ and critically analyses if their digital privacy interests are adequately protected by data privacy law and the practices of videogame websites.

On 23rd June 2016, the UK voted to leave the European Union in the ‘United Kingdom European Union membership referendum’ (also known as the EU referendum and the Brexit referendum) by 52% to 48%.⁴⁴ Article 50 of the Treaty of Lisbon outlines the right of an EU member state to quit unilaterally and the procedure to do so. Prime Minister Theresa May began the formal process of departing from the EU by triggering Article 50 on 29th March 2017.⁴⁵ The two-year process is due to complete next March 2019, and the UK will exit the EU.

For this thesis, it is important to consider the effects of Brexit on the EU GDPR 2018.⁴⁶

The European Communities Act 1972, which implements EU law into UK, will become

⁴³ Children’s online privacy and freedom of expression (UNICEF May 2018) [https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf) accessed 17 November 2018.

⁴⁴ EU referendum results (The Electoral Commission) < <https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information>> accessed 18 June 2018; ‘Results’ (BBC News) <http://www.bbc.co.uk/news/politics/eu_referendum/results> accessed 16 May 2017. Following on from this result, there has been a lot of discussion around issues including a backlash to globalisation, inequality, a possible divide between city and rural areas and the future relationship of Britain with the EU and the rest of the world. ‘After Brexit: Britain’s Future’ (Chatham House) <<https://www.chathamhouse.org/research/regions/europe/UK/after-brexit-britain-future?page=1#fragment-0>> accessed 16 May 2017; House of Lords European Union Committee, ‘Brexit: The EU Data Protection Package’ (parliament.uk 18 July 2017) <<https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf>> accessed 22 January 2018.

⁴⁵ Alex Hunt and Brian Wheeler, ‘Brexit: All You Need to Know about the UK Leaving the EU’ (BBC News, 25 April 2017) <<http://www.bbc.co.uk/news/uk-politics-32810887>> accessed 16 May 2017.

⁴⁶ ‘Reform of EU Data Protection Rules’ (Europa) http://ec.europa.eu/justice/data-protection/reform/index_en.htm accessed 16 May 2017.

redundant.⁴⁷ The next section will consider the impact of Brexit for the EU GDPR 2018.

1.1.2. Impact of Brexit

By way of background, the UK became a member of the EU on 1st January 1973.⁴⁸ The Data Protection Directive 95/46/EC⁴⁹ was adopted by the EU in 1995. It was the first EU based data protection and privacy law to protect the processing and free movement of data belonging to EU citizens. This Directive was no longer in force on 24th May 2018 having been replaced with the new EU GDPR 2018 on 25th May 2018 in the EU.

The European Union (Withdrawal) Bill (also known as the Repeal Bill or the Great Repeal Bill),⁵⁰ will repeal the European Communities Act 1972 and will implement the UK's exit from the EU and remove the competence of EU institutions to legislate for the UK. It also provides that all directly applicable and already existing EU law will still be transposed into the UK, creating a new category of UK laws called 'retained EU law'.⁵¹ This means that the provisions of the EU GDPR 2018 will remain part of UK law through clause 3 of the Repeal Bill if it becomes law.

⁴⁷ European Communities Act 1972 Section 2.

⁴⁸ United Kingdom (Europa) < https://europa.eu/european-union/about-eu/countries/member-countries/unitedkingdom_en > accessed 22 June 2018.

⁴⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

⁵⁰ European Union (Withdrawal) Bill (HC Bill 5) < https://publications.parliament.uk/pa/bills/cbill/2017-2019/0005/cbill_2017-20190005_en_1.htm > accessed 22 January 2018.

⁵¹ European Union (Withdrawal) Bill (HC Bill 5) Sections 2–6.

The UK government intends that UK data protection law should mirror EU law to facilitate transborder data flows.⁵² As a consequence, the Data Protection Bill was introduced into the House of Lords on 13 September 2017, which replicates the Data Protection Act 1998 as far as possible.⁵³ It received Royal Assent on 23rd May 2018 and is now the Data Protection Act 2018.⁵⁴ The Act aims to modernise data protection laws in the UK in years to come. According to the UK Information Commissioner's Office ('UK ICO'), both EU GDPR 2018 and the Data Protection Act 2018 should be read side by side.⁵⁵ This is because EU GDPR 2018 has direct effect across all EU member states but there are limited provisions on how it applies in member states. The Data Protection Act 2018 will provide details on this as well as areas that do not fall within EU law such as immigration and national security.⁵⁶

Although the Data Protection Act 2018 is broader than the EU GDPR 2018, it largely replicates the new EU GDPR 2018. The EU GDPR 2018 has extraterritorial effect. It will certainly apply to data processing in the UK after Brexit. But it will complement the Data Protection Act 2018. The Act treats children as a special class of data subjects because it provides for the age of consent as 13 years (*see 1.2.3; 4.10.1; 8.2.1*).⁵⁷

The House of Lords has expressed concern about the lack of detail on how the government plans to achieve Brexit. The EU's Charter of Fundamental Rights and

⁵² John Woodhouse and Arabella Lang, 'Brexit and Data Protection' (House of Commons Library, 10 October 2017) <<file:///C:/Users/User%201/Downloads/CBP-7838.pdf>> accessed 22 January 2018.

⁵³ Data Protection Bill [HL] 2017-19 <<https://services.parliament.uk/bills/2017-19/dataprotection.html>> accessed 22 January 2018.

⁵⁴ Data Protection Act 2018 (www.parliament.uk) <https://services.parliament.uk/bills/2017-19/dataprotection.html> accessed 17 June 2018.

⁵⁵ Data Protection Act 2018 (ico) < <https://ico.org.uk/for-organisations/data-protection-act-2018/>> accessed 17 June 2018.

⁵⁶ *Ibid.*

⁵⁷ Data Protection Act 2018 Section 9(a).

Freedoms will be removed from retained EU law.⁵⁸ Article 8 of the Charter has been interpreted to mean that individuals should have the right to protect their personal data. There are two key concerns; how can UK ensure compliance with data protection laws without reference to Article 8 rights under the Charter; and can there be close cooperation between UK and EU on exchanging data, in the absence of the principles relied on in the Charter? These still need to be resolved and are not discussed further on in this thesis.

This thesis will carry out a two-part multiple case study. The first part will analyse the privacy policies of 10 videogames.⁵⁹ The second part of the study will examine the same privacy policies with respect to governing data privacy laws.⁶⁰ In particular, the thesis will consider the compatibility of rules and practice with the expectation for children to read, understand and consent to privacy policies.

The study will identify any gaps that need to be addressed to protect children's digital privacy rights. The most important contribution of this thesis will be an original child-friendly model privacy policy⁶¹ that will be brief, easy to understand and child-friendly.

1.2. Background to the problem

1.2.1. Internet and data tracking techniques

⁵⁸ John Woodhouse and Arabella Lang, 'Brexit and Data Protection' (House of Commons library 10 October 2017) <<file:///C:/Users/User%201/Downloads/CBP-7838.pdf>> accessed 22 January 2018.

⁵⁹ Chapter 5 Part 1 – Online games case studies: Privacy policies and children.

⁶⁰ Chapter 6 Part 2 – Online games case study: Privacy policies and governing data privacy law.

⁶¹ Chapter 7 – Original child-friendly model privacy policy.

Personal data has been referred to as ‘gold nuggets’ by Florin Gorunescu for its priceless utility in the modern age of online commerce.⁶² Rapid technological changes, quick development of the internet, electronic commerce and sophisticated methods of collecting, analysing and using personal information have made digital privacy problematic.⁶³

Children carry out a host of activities on the internet, which include but are not limited to using social media and search engines and playing videogames. Tens of petabytes⁶⁴ of data are created daily. This data is sifted utilising intelligent techniques that highlight interesting patterns, which in turn serve to advance lucrative commercial interests by mapping demographic patterns and behavioural profiles of website visitors. The information helps organisations gain a competitive edge, adopt more efficient business practices and deliver customised new products to online users.⁶⁵

The thesis is divided into two main parts: the comparative law study⁶⁶ and the two-part multiple case study.⁶⁷ Key findings of the comparative study confirms online consent is unreliable and difficult to prove (*see 4.10.3*); varying ages for online

⁶² Florin Gorunescu, *Data Mining Concepts Models and Techniques* (Springer 2011).

⁶³ Dileep Kumar Singh and Vishnu Swaroop, ‘Data Security and Privacy in Data Mining: Research Issues & Preparation’ (2013) 41(2) *IJCTT* 194.

⁶⁴ Computer technology storage units of measurement are based on the byte, and 1 petabyte is equal to one quadrillion bytes. Tim Fisher, ‘Terabytes, Gigabytes, & Petabytes: How Big are They?’ (Lifewire, 20 September 2017) <<https://webcache.googleusercontent.com/search?q=cache:o8KdFrGKADEJ:https://www.lifewire.com/terabyte-s-gigabytes-amp-petabytes-how-big-are-they-4125169+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 27 October 2017.

⁶⁵ Sonia Livingstone and Leslie Haddon, ‘Introduction-Kids Online: Opportunities and Risks for Children’ (Policy Press 2009) <[http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_\(LSERO\).pdf](http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf)> accessed 23 January 2016.

⁶⁶ Chapter 3 – The current European digital privacy legislation; Chapter 4 – Data protection and privacy framework in the U.S. and Canada.

⁶⁷ Chapter 5 Part 1 – Online games case studies: privacy policies and children; Chapter 6 Part 2 – Online games case studies: privacy policies and governing data privacy law.

consent in different legislatures fail to comply with international agreements that define a child as anyone under the age of 18 years,⁶⁸ (see 4.10.1) creating diverging data protection and privacy practices. The need for data privacy law to have clarity on children's digital privacy concerning the collection, processing and potential disclosure of their personal data; and the need for data protection authorities to be strengthened and empowered to take enforcement action against perpetrating organisations (see 4.10.4).

The two-part multiple case study firstly identifies that there are readability issues for children expected to read privacy policies and lack a standard (see 5.5.2). Websites collect extensive information from children while failing to comply with data privacy principles of minimality⁶⁹ (see 3.2.3.3) and purpose specification⁷⁰ (see 3.2.3.2; 5.5.6 & 5.5.7; 6.2.6 & 6.4.4) Some of the privacy policies imply consent, which contravenes the legal definition for consent to be a specific, positive and informed action on the part of the user⁷¹(see 5.5.10). Finally, methods to disable cookies are complicated (see 5.5.8 & 5.5.9) and users are unaware of the specific law that governs the terms of the privacy policy (see 6.2.3).

1.2.2. Videogame websites collect personal information from digital users

Academics have pointed out that there is a lack of research on the types of harm to children that may arise from data tracking and user monitoring tools that are built

⁶⁸ Most countries are signatories to the UN Convention on the Rights of the Child, which defines a child as anyone under the age of 18 under Article 1.

⁶⁹ Directive 95/46/EC Article 6(1)(c): Data should be adequate, relevant and not excessive to the purposes for which they are collected and/or processed; EU GDPR 2018 Article 5(1)(c).

⁷⁰ Directive 95/46/EC Article 6(1)(b): Data should be gathered for a specified, legitimate and compatible purpose; EU GDPR 2018 Article 5(1)(b).

⁷¹ Directive 95/46/EC Article 2(h).

into commercial platforms.⁷² Given that children are expected to consent to privacy policies, they should be able to understand the legal consequences of giving consent⁷³ (see 5.5.2.4). There is, however, research on the psychological attributes of adolescence that can help us in understanding the vulnerabilities that teens can face in data collection.⁷⁴ According to Eleni Kosta, and Milda Macenaite, processing of children's personal data can entail security risks including commercial exploitation and misuse of personal data, profiling, identity theft, the loss of reputation, and discrimination.⁷⁵

According to IDAnalytics, a risk management firm, each year more than 140,000 children are at risk of identity theft in the U.S.⁷⁶ Videogames can increase the chances of children's identity theft because they may not read the fine print of the company's terms and conditions for use and may easily divulge personal information, and parents could fail to ensure appropriate privacy settings.⁷⁷

Children may be less capable of evaluating perilous situations. They may easily be misled and exploited by online marketers that collect personal data and employ

⁷² Belinha S. De Abreu and others, *International Handbook of Media Literacy Education* (Routledge 2017).

⁷³ Dawn Watkins and others, 'Exploring Children's Understanding of Law in Their Everyday Lives (2018) 38(1) Legal Studies. Data Research into a person's understanding of law-related issues and the ability to deal effectively with them has focused primarily on adults.

⁷⁴ Cornelia Pechmann and others, 'Impulsive and Self-Conscious: Adolescents' Vulnerability to Advertising and Promotion' (2005) 24(2) *Journal of Public Policy & Marketing* 202.

⁷⁵ Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) *Information & Communications Technology Law* 146.

⁷⁶ 'More than 140,000 Children Could Be Victims of Identity Fraud Each Year' (id:analytics, 12 July 2011) <<http://www.idanalytics.com/press-release/140000-children-victims-identity-fraud-year/>> accessed 28 October 2017.

⁷⁷ Kate Rogers, 'Video Games Could Increase Children's Risk of Identity Theft' (Fox News, 31 August 2011) <<http://www.foxbusiness.com/features/2011/08/31/video-games-could-increase-childrens-risk-identity-theft.html>> accessed 28/10/2017; *League of Legends* is a popular 'battle arena' game that suffered a major security breach in 2013 when it exposed account information of its North American players including first and last names, passwords and email addresses. The breach also released transaction records such as encrypted credit card numbers from as early as 2011. Rob Waugh, 'League of Legends Players Warned after Major Security Breach' (welivesecurity 22 August 2013) <<https://www.welivesecurity.com/2013/08/22/league-of-legends-players-warned-after-major-security-breach/>> accessed 28 October 2017.

special techniques and ‘dynamic creative’ ads tailored to their individual profile and behavioural patterns.⁷⁸

When children visit a videogame website, they become voluntary and involuntary contributors of their personally identifiable information. They are highly encouraged to register, or else they may not be able to access key services offered by the videogame publisher. While registering, they provide their personal information such as their full name, date of birth, gender, email address and in some instances their parents’ financial or bank card details.

Children’s vulnerability online necessitates a special case

The EU GDPR has acknowledged the relative vulnerability that can be demonstrated by children when interacting with the online community⁷⁹ and introduced special provisions for children, regarded as deserving additional protection online.⁸⁰ This approach is not unique as there are other legal frameworks which have recognised that children need additional protection. For example, in the UK the Advertising Standards Authority (‘ASA’) and Committee of Advertising Practice (‘CAP’) acknowledge that children react differently to marketing communications influenced by their age and experience.⁸¹ Therefore, under the CAP code children under 16 years should not be subject to direct marketing communication that appeals to them to buy advertised products, take risks, copy unsafe undesirable practices, be presented

⁷⁸ Ibid.

⁷⁹ EU GDPR Recitals 38 and 75

⁸⁰ EU GDPR Article 8 (parental consent required for children under 16 years of age); Article 22(1) (restriction on automated processing of children’s data).

⁸¹ Children: general (Advertising Standards Authority 17 July 2018) < <https://www.asa.org.uk/advice-online/children-general.html> > accessed 1/12/2018.

with images depicting violence or sex.⁸² The ASA has taken special measures in a medium where children are not directly interacting with advertising content. The online medium however requires children to interact on a more personal level. They are expected to submit some part of their personal data in return for using a website's services. Additionally, children may demonstrate varying levels of maturity online. The CAP code is an example of a legal framework where the age of consent is relatively high, which is arguably justified in view of the additional risks online.

Another example relates to medical consent and the concept of 'Gillick competency',⁸³ under which children under 16 years are not legally competent to give medical consent unless they are medically judged to have 'sufficient understanding and maturity to enable them to understand fully what is proposed'.⁸⁴ However this concept does not map easily on to the digital environment. In digital media, there is no physical interaction between children and the website operator to determine if they have the required maturity to online consent. With the associated risks, it may be in the best of interests of a child to set a higher age at which children can provide digital consent.

While interacting with the online community, children can be subjected to a number of digital privacy risks including inappropriate content. During the process of selecting videogames for the multiple case study in this thesis, the researcher came across adult content including semi-nude animated characters and gambling games in

⁸² Ibid; UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code)

⁸³ Claire A. Williams and Russell Perkins, *Consent Issues for Children: A Law unto Themselves?* (2011) 11(3) BJA 99

⁸⁴ *Gillick v West Norfolk & Wisbeck Area Health Authority* [1986] AC 112 House of Lords.

Miniclip⁸⁵ with an age restriction of 11+. Even though the EU GDPR has set the age of consent at 16 years, the online world is practically borderless and heavily unregulated, allowing children to access all kinds of content at the touch of a button. The selection of the age of consent at the upper limit of 18 years would help to avoid children being exposed to undesirable content.

This protectionist approach is also justified by psychological studies that suggest adolescents are more vulnerable online than adults owing to their behavioural characteristics, emotional volatility and impulsiveness which may increase vulnerability to addictive behaviour.⁸⁶ Such non-substance or 'behavioural addictions' can directly result from activities including internet use and videogames.⁸⁷ Developmental changes during the period of adolescence can contribute towards poor choices to achieving immediate rewards which increases between the ages of 14-18 years.⁸⁸ It is suggested that although children develop learning and understanding abilities at the age of 16 years, decisions that can influence/not influence poor choices will depend on the extent of information available to the data subject.⁸⁹ Hence, only where the website presents all information in easy to understand and child-friendly language, can a child above 16 years of age provide digital consent. In the absence of such information and with the largely unregulated

⁸⁵ <<http://www.miniclip.com/games/en/>> accessed 1 December 2018. Miniclip is a free to play online videogame with a collection of games.

⁸⁶ Judith Bessant, 'Hard Wired for Risk: Neurological Science, "the Adolescent Brain" and Developmental Theory' (2008) 11(3) *Journal of Youth Studies* 347, 358. Adolescence typically refers to the years between 13 and 19 years and can be considered the transitional stage from childhood to adulthood.

'Adolescence' <<https://www.psychologytoday.com/basics/adolescence>> accessed 3 December 2017. For the reason behind selecting the age of 18 years; 'Digital Heroin: Is the Internet REALLY a Drug? [Debate]' (ICDL Arabia, 14 February 2017) <<http://webcache.googleusercontent.com/search?q=cache:Z4a6-VBWgxIJ:onlinesense.org/digital-heroin/+&cd=4&hl=en&ct=clnk&gl=uk>> accessed 18 January 2018.

⁸⁷ Kornelia N. Balogh, Linda C. Mayes and Marc N. Potenza, 'Risk-taking and decision-making in youth: relationships to addiction vulnerability [2013] *J Behav Addict* 12(1)

⁸⁸ Ibid.

⁸⁹ Ibid.

online environment, adolescents could be at risk of making poor and risky choices towards protecting themselves against digital privacy risks.

There are a number of situational and psychological factors that can determine a child's maturity and mental capacity to consent. In consideration of the above, children should first be provided with a safe and protected digital environment to interact with. Once this is done, children should then be provided with the tools to empower and protect themselves against digital privacy risks (*see section 1.1*)

1.2.3. What is the optimal age for consent?

Children's personal data (directly identifiable information)⁹⁰ arguably needs special protection online. Although the EU GDPR 2018 provides special rules for children, member states can reduce the age of consent from 16 to 13 years.⁹¹ While giving regard to the various approaches towards choice of age for consent, this thesis adds a protectionist perspective to this discussion by proposing the age of 18 years for a child in relation to online videogames (*see 4.10.1; 6.4.8; 7.3.1.2; 8.2.1*). UN Convention on the Rights of the Child ('UNCRC') is one of the most important international legal frameworks for children's rights.⁹² Article 1 UNCRC defines a child as anyone under the age of 18 years unless a particular country sets a lower legal age for adulthood. This means that UNCRC has allowed signatories to take account of cultural variations when making this choice.⁹³ But the Committee encourages states

⁹⁰ EU GDPR 2018 Article 4

⁹¹ EU GDPR 2018 Article 8.

⁹² UN Convention on the Rights of the Child Article 1; United Nations treaty collection <https://webcache.googleusercontent.com/search?q=cache:nr6kif9nff4J:https://treaties.un.org/Pages/ViewDetails.aspx%3Fsrc%3DIND%26mtdsg_no%3DIV-11%26chapter%3D4%26lang%3Den+&cd=1&hl=en&ct=clnk&gl=uk> accessed 14 April 2018.

⁹³ Fact sheet: A summary of the rights under the Convention on the Rights of the Child (UNICEF) https://www.unicef.org/crc/files/Rights_overview.pdf accessed 16 November 2018.

to review the age of majority if it is set below 18 and to increase the level of protection for all children under 18.⁹⁴

In the UK, the age of consent for a child is 16 years,⁹⁵ which could also be accepted as the age for giving online consent under the EU GDPR 2018. However, the Data Protection Act 2018 has recently set the age for online consent at 13 years.⁹⁶ This means that children will be treated as a special class of data subjects, but this creates confusion. The EU GDPR 2018 has set the age for consent as 16 years but allowed member states the option to reduce this age to 13 years.⁹⁷ This means that member states will adopt their own interpretation of age for consent leading to uncertainty in the law. In the U.S., the Children's Online Privacy Protection Act refers to a child as anyone under the age of 13 years.⁹⁸ In the U.S., websites directed towards children under 13 years will require verifiable parental consent,⁹⁹ while children aged 14 to 17 years will be treated as adults that are expected to read, understand and consent to privacy policies. One other reason for including individuals aged 14-17 years within the definition of 'child' is studies suggesting adolescents are more vulnerable online than adults owing to their behavioural characteristics, emotional volatility and impulsiveness¹⁰⁰. The EU GDPR also refers to children as vulnerable natural persons

⁹⁴ Ibid.

⁹⁵ England and Scotland in the Sexual Offences (Amendment) Act of 2000.

⁹⁶ Data Protection Act 2018 Section 9(a).

⁹⁷ EU GDPR 2018 Article 8.

⁹⁸ [Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505](#); 16 CFR §312.2

⁹⁹ [Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505](#) §6501(1). According to the European Commission, verifiable parental consent is required from children under 13 years of age. 'Children's Data Protection and Parental Consent (Advertising Education Forum October 2013) <<http://www.aeforum.org/gallery/5248813.pdf>> accessed 7 February 2018.

¹⁰⁰ Judith Bessant, 'Hard Wired for Risk: Neurological Science, "the Adolescent Brain" and Developmental Theory' (2008) 11(3) *Journal of Youth Studies* 347, 358. Adolescence typically refers to the years between 13 and 19 years and can be considered the transitional stage from childhood to adulthood.

'Adolescence' <<https://www.psychologytoday.com/basics/adolescence>> accessed 3 December 2017. For the reason behind selecting the age of 18 years; 'Digital Heroin: Is the Internet REALLY a Drug? [Debate]' (ICDL Arabia, 14 February 2017) <<http://webcache.googleusercontent.com/search?q=cache:Z4a6-VBWgxlJ:onlinesense.org/digital-heroin/+&cd=4&hl=en&ct=clnk&gl=uk>> accessed 18 January 2018.

in Recital 75 that maybe exposed to risks of varying severity leading to harm where personal data processing can reveal sensitive information.

This thesis also acknowledges that children under 16 years should provide parental consent. This will remain compatible with the EU GDPR 2018 requirement that parental consent is needed when processing personal data of children under 16 years.¹⁰¹

1.2.4. Parental consent

In the EU GDPR, consent must be freely given, specific, informed, written and an unambiguous indication of a data subject's wishes.¹⁰² In the U.S., the Children's Online Privacy Protection Act ('COPPA')¹⁰³ requires verifiable parental consent¹⁰⁴ before website operators can collect and process personal data belonging to children under 13 years¹⁰⁵ (see 4.3.3.2 & 4.10.3) COPPA defines verifiable parental consent as any reasonable effort to ensure that a parent receives notice and authorises the operator's personal information collection, use, and disclosure practices of information collected from a child.¹⁰⁶

The Federal Trade Commission ('FTC')¹⁰⁷ provides a list of methods to obtain parental consent but they are not entirely verifiable. This is because it is difficult to prove the

¹⁰¹ EU GDPR 2018 Article 8(1).

¹⁰² Article 7 and Recital 32 EU GDPR

¹⁰³ [Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.](#)

¹⁰⁴ The term 'verifiable parental consent' has not been defined by the Data Protection Directive 95/46/EC or the EU GDPR 2018.

¹⁰⁵ COPPA Section 6501(1) and (9).

¹⁰⁶ COPPA Section 6501(9).

¹⁰⁷ The Federal Trade Commission is a federal agency in the U.S. that protects consumers by stopping unfair, deceptive or fraudulent practices in the marketplace. It collects complaints of hundreds of issues from data security and deceptive advertising to identity theft. Federal Trade Commission, 'What We Do' (FTC) <<https://www.ftc.gov/about-ftc/what-we-do>> accessed 14 March 2018.

identity of the person giving consent (*see 3.2.5.3; 5.5,10.2; 6.2.9 & 6.4.3 & 6.6.5*). For instance, in the email plus method¹⁰⁸ children can provide a fictitious email address and consent can be provided without necessarily involving parents or responsible adult. Additionally, not everyone has a responsible parent and children in the care system may not have access to individuals undertaking sufficient parental responsibility (*see 4.10.3*).

Consent will authorise websites' collection of user's personal information including through smart tracking technologies such as cookies.¹⁰⁹ Users have the choice to opt out of tracking, but it can be a complicated process. Suffice to say that a digital profile is created of visitors, where each click, movement and split-second decision they make is tracked,¹¹⁰ and potentially disclosed to third parties across vast spans of commercial interests. If a parent must give their consent to their child's use of videogames, they should be able to understand the consequences of giving consent: that their children's personal data will be subject to the website's data handling practices. If parents do not have the requisite knowledge to understand the workings of the digital environment, this may not be the case. Indeed, the concept of parental consent is fraught with issues. Studies suggest that children place a strong degree of trust and confidence in their adults to resolve issues.¹¹¹ Additionally, this trust can be

¹⁰⁸ 16 C.F.R. § 312.5(b)(2) Under the 'email plus' method, the website operator will send an email to the parent and have them respond with their consent. A confirmation of the consent will be sent to the parent via email, letter, or phone call and the parent must be able to revoke consent at anytime.

¹⁰⁹ Cookies are small text files that are downloaded onto a user's computer or smartphone when they visit a website. It helps to remember users' devices as well as store information about their preferences or past actions 'Cookies and Similar Technology' (ICO) <<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>> accessed 18 March 2017.

¹¹⁰ [Éloïse Gratton](#), *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (CCH Canada Ltd 2003).

¹¹¹ Watkins and others, 'Exploring Children's Understanding of Law in Their Everyday Lives (2018) 38(1) Legal Studies.

misplaced when it comes to legal issues as most (adults) people in the UK lack legal knowledge of their legal rights. If consent is relied on as a legitimate basis for processing, parents are an important part of the process to provide verifiable parental consent. According to the EU GDPR, consent should be an informed indication of the data subject's wishes. Parents should be aware of the rights and obligations their children are entitled to under the terms of the privacy policy. For this reason, the draft child-friendly privacy policy (*see section 7.7*) provides a link to the governing data privacy law which is presented in simple and easy to understand language. Issues can still arise if parents don't have an adequate supervisory role, are absent or if the child is in local authority care. (*see 4.10.3*). In such instances, it is essential to provide children with a safe and protected digital environment.

It is important for digital environments to be well regulated and controlled to create a healthy atmosphere conducive to learning and entertainment.¹¹² Parents (or those with legal responsibility) should be able to provide a verifiable consent by indicating an express, informed and unambiguous indication of their wishes.

The UK Information Commissioner's Office (ICO)¹¹³ published guidance on the requirements of consent under the EU GDPR 2018.¹¹⁴ It states, if valid consent cannot be obtained, the principles of fair data processing should be relied upon as an alternative legal basis for processing.¹¹⁵ In other words, website operators should

¹¹² 'The Protection of Children Online' (OECD, 2012)

<https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf> accessed 21 February 2018.

¹¹³ ICO <<https://ico.org.uk/for-the-public/>> accessed 29 April 2018. The Information Commissioner's Office (ICO) is the UK's independent authority that protects data privacy rights/information rights in the public interest.

¹¹⁴ 'ICO GDPR Guidance' (ICO 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017.

¹¹⁵ Ibid.

depend on data protection principles of minimality,¹¹⁶ transparency and purpose specification¹¹⁷ to ensure safety for children’s digital privacy. Website operators should collect children’s personal data that is strictly limited to the specified purposes for collection. A strong data protection and privacy law is required that is adequate, relevant and not excessive users feel overwhelmed.

The EU GDPR 2018 requires consent in the ‘context of a written declaration’ for the processing of personal data,¹¹⁸ which means that website visitors will be subject to repeated consent messages,¹¹⁹ leading to ‘consent transaction overload.’¹²⁰

The law should be able to regulate the practices of websites to ensure they can maintain a balance between the digital privacy rights of users on the one hand and on the other the commercial advantage to the organisation of collecting and understanding market patterns.

1.3. Literature

It is important to consider the existing research works in the field of videogames and data surveillance. One of the earliest works was carried out by Easwar A. Nyshadham, a professor at Nova Southeastern University,¹²¹ in his article ‘Privacy Policies of Air

¹¹⁶ Directive 95/46/EC Article 6(1)(c): The principle of minimality limits data collection so that it is adequate, relevant and not excessive; Directive 95/46/EC Recital 28; Chapter 3 Section 3.2.3.3; EU GDPR 2018 Article 5(1)(c).

¹¹⁷ Directive 95/46/EC Article 6(1)(b): For the principle of ‘purpose specification’, data should be gathered for a specified, legitimate and compatible purpose; Chapter 3 Section 3.2.3.2; EU GDPR 2018 Article 5(1)(b).

¹¹⁸ EU GDPR 2018 Articles 4(11) and 7(2).

¹¹⁹ Christine Jolls and Cass R. Sunstein, ‘Debiasing through Law’ (2006) 35(1) *The Journal for Legal Studies* 199, 212.

¹²⁰ The strict legal requirements of consent will lead to repeat consent requests and pop ups that will desensitize the purpose of consent. Bart W. Schermer, Bart Custers and Simone Van Der Hof, ‘The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection’ (2014) 16(2) *Ethics Info Technol* 171, 176–178.

¹²¹ <<http://www.ratemyprofessors.com/ShowRatings.jsp?tid=433413>> accessed 8 December 2017.

Travel Web Sites: A Survey and Analysis',¹²² where he studied the privacy policies of 23 airlines to determine if they are compatible with the four principles of fair information practices (notice, choice, access and security). The results revealed very few firms in the airline travel industry complied with these principles, especially through incorporating steps to provide security for information both during transmission and after their sites receive the information.

The most prominent research works in the field of videogame websites and issue of privacy was carried out in 2005 by Professor Sara M. Grimes and Grace Chung in 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games'.¹²³ They realised the elevated importance offered to individuals' personal information but found that little if any attention is paid to information that is collected and electronically scanned for commercial reasons. They researched the contents of the End User Licence Agreements (EULAs) of some of the most popular children's game sites. Their paper demonstrates how data gathering practices can threaten the digital privacy rights of children, which can be highly valued in the marketing industry. The authors reviewed current online market research trends, data gathering techniques and policy initiatives.

There is limited research in commercial exploitation of children's digital data with respect to videogame websites. An important article in this area was published in May 2017 co-written by Milda Macenaite and Eleni Kosta, who highlight the digital profiling of children and critically analyse the provisions of the EU GDPR 2018 in

¹²² Easwar A. Nyshadham, 'Privacy Policies of Air Travel Websites: A Survey and Analysis' (2000) 6(3) Journal of Air Transport Management 143.

¹²³ Grace Chung and Sara M. Grimes, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2005) 30(4) Canadian Journal of Communication.

regulating children's consent.¹²⁴ It is one of the few articles that acknowledges the commercial exploitation of children (and teenagers) resulting from the unscrupulous data handling practices of websites. The article also explores the effects of the EU GDPR 2018 on the data privacy rights of children and compares it with the provisions of COPPA.

Also in 2017, the relationship between data protection law and the right to privacy was examined by Maria Tzanou in her book, *The Fundamental Right to Data Protection*.¹²⁵ She examined four case studies of counterterrorism-related surveillance that have led to massive profiling of individuals across the world. She identified that courts are more inclined to rule a case based on an abrogation of the right to privacy rather than data protection by evaluating communications metadata surveillance, travel data surveillance, financial data surveillance and internet data surveillance. Tzanou's research helps to develop a better understanding of the normative value of data protection as an autonomous right.

There are numerous additional, less rigorous, publications such as government reports, blogs and news articles that have highlighted the importance of protecting children's rights to digital privacy. Anne Longfield, Children's Commissioner for England, published a report called 'Growing Up Digital'.¹²⁶ The report provides that children are 'left to fend for themselves in the digital world'; they do not understand the terms and conditions they agree to; they end up submitting their personal data

¹²⁴ Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) Information & Communications Technology Law 146.

¹²⁵ Maria Tzanou, *Fundamental Right to Data Protection* (Bloomsbury Publishing 2017).

¹²⁶ Children's Commissioner, 'Growing Up digital' (The Children's Commissioner's Office) <<https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/>> accessed 13 January 2018.

and expose themselves to online abuse'.¹²⁷ She proposes the creation of a new 'digital ombudsman' to uphold the rights of children under 18 years on the internet, a digital citizenship programme that is compulsory in schools from four to 14 years, and simplifying terms and conditions for digital services offered to children.¹²⁸ In November 2017, Parliament backbencher and film director Baroness Beeban Kidron¹²⁹ (*Chapter 8 Section 8.4*) proposed amendments to the UK's Data Protection Bill 2017,¹³⁰ calling for technology companies to be subject to 'minimum standards of age-appropriate design' so as to control advertising and notifications that allow for endless data gathering, posing a risk of personal information being disseminated online.¹³¹ The Council of Europe has increased calls to transform children's rights, in particular rights guaranteed by the UN Convention on the Rights of Child to cater for the 'digital age'.¹³² The Bill received Royal Assent on 23rd May 2018 and is now the Data Protection Act 2018¹³³ (*see 1.1.2*)

¹²⁷ Ibid.

¹²⁸ Ibid.

¹²⁹ 'Baroness Beeban Kidron' (The Children's Media Conference)

<<http://www.thechildrensmediakonference.com/profile/baroness-beeban-kidron/>> accessed 20 April 2018.

Baroness Kidron is a British filmmaker who has made films including *Bridget Jones: The Edge of Reason*. In 2012 she was appointed as a crossbencher in the House of Lords and is founder of 5Rights, a campaign to deliver digital rights to children.

¹³⁰ The Data Protection Bill will update data protection laws for the digital age and was introduced in the House of Lords on 13 September 2017. The Data Protection Bill 2017

<<https://www.gov.uk/government/collections/data-protection-bill-2017>> accessed 14 January 2018.

¹³¹ Anushka Asthana, 'Lords Push for New Regulations to Protect Children Online' *The Guardian* (London, 18 November 2017) <<https://www.theguardian.com/society/2017/nov/18/lords-push-for-children-to-be-protected-against-tech-giants-by-law>> accessed 14 January 2018.

¹³² 'Council of Europe Strategy for the Rights of the Child (2016–2021)' (Council of Europe, March 2016).

<<https://rm.coe.int/168066cfff8>> accessed 3 December 2017; UN Committee on the Rights of the Child, Report of the 2014 Day of General Discussion "Digital Media and Children's Rights" (OHCHR)

<http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf> accessed 3 December 2017.

¹³³ Data Protection Act 2018 (www.parliament.uk) <https://services.parliament.uk/bills/2017-19/dataprotection.html> accessed 17 June 2018.

EU Kids Online reported on the analytical model to research children's online risks and opportunities.¹³⁴ To understand risks online one should inquire into both the nature of the providers (the producers, participants and designed structures that constitute the online environment) and the agency and diversity of children's roles in engaging with these.¹³⁵ This thesis will discuss how children can be treated as a special class of data subjects when playing online videogames.

The original contribution to knowledge of this thesis is that it is the first legal study examining the privacy issues in relation to data gathering practices employed in popular videogames. It also examines the adequacy and effectiveness of legislation for data protection and privacy in selected international legislatures, from the perspective of children's digital privacy rights.

The study will build on the concept of digital privacy, which has been examined by numerous scholars, with respect to children's privacy rights when they play videogames online.¹³⁶ This thesis will carry out a legislative analysis by considering the effectiveness of data privacy laws in the EU, the U.S. and Canada in regulating videogame privacy policies and protecting children's digital privacy rights from commercial exploitation.¹³⁷

¹³⁴ Sonia Livingstone, Giovanna Mascheroni and Elisabeth Staksrud, 'Developing a Framework for Researching Children's Online Risks and Opportunities in Europe' (EU Kids Online, November 2015) <http://eprints.lse.ac.uk/64470/1/_lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU%20Kids%20Online_Developing%20framework%20for%20researching_2015.pdf> accessed 3 December 2017.

¹³⁵ Ibid.

¹³⁶ France Belanger and Robert E. Crossler, 'Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems (2011) 35(4) MIS Quarterly 1017; Maria Tzanou, *Fundamental Right to Data Protection* (Bloomsbury Publishing 2017).

¹³⁷ Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) Information & Communications Technology Law 146.

This two-part multiple case study will determine if data handling practices remain compatible with governing data privacy laws. First, it interrogates the privacy awareness of online users by consulting reports and surveys carried out by EU Kids Online,¹³⁸ followed by a detailed investigation of the contents of privacy policies of 10 videogame websites, which have been selected based on their popularity ranking as recorded in 2015. Based on the findings of the comparative legislative analysis and multiple case study, the original child-friendly model privacy policy will be presented that will address any shortcomings observed in the study.

1.4. Significance of the study

*'Giving children the tools to protect themselves against threats on the Internet ... is probably the most effective way of safeguarding children's rights on the Internet ... it is even more important to act preventatively by raising their awareness about potential risks and long-term consequences of sharing personal information on the Internet.'*¹³⁹

Children can make independent choices if they have the requisite skills to make prudent choices and are empowered to do so. There is substantial divergence in Europe on when children are competent to make decisions.¹⁴⁰ In Denmark and Slovenia, medical consent is given at the age of 15 years; 16 years in Spain¹⁴¹ and England.¹⁴² In England, under the Sexual Offences Act 2003, children can give legal consent to sex at the age of 16; and children aged 13 years are entitled to work part-

¹³⁸ EU Kids Online (LSE) <<http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online>> accessed 29 April 2018. EU Kids Online is a multinational research network that explores parents and children's experience of the internet to help in the dialogue with national and European policy stakeholders.

¹³⁹ Commissioner for Human Rights, 'Protecting Children's Rights in the Digital World: An Ever-Growing Challenge' (Europa, 29 April 2014) <<https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1?desktop=true>> accessed 7 February 2018.

¹⁴⁰ Cave, Emma, 'Adolescent consent and confidentiality in the UK.' [2009] European journal of health law., 16 (4).

¹⁴¹ Stultiens, L., T. Goffin, P. Borry, K. Dierickx, H. Nys, 'Minors and Informed Consent: A Comparative Approach' European Journal of Health Law, 14 (2007).

¹⁴² Section 8 (1) of the Family Law Reform Act 1969.

time.¹⁴³ In the digital environment, there is no fixed age at which children can give consent. The EU GDPR provides that children aged 16 are competent to give legal consent and allows member states the option to reduce this age to 13 years.¹⁴⁴ Additionally, digital consent is provided without physical presence or assessment of the child's maturity. Studies indicate that children should be made aware of digital risks so that they can be empowered to use the tools to protect themselves online (*see footnote 3*) Therefore, this thesis adopts the approach that to raise awareness among children of the risk presented in the digital environment, a preventative process should be used in this specific context. Children under 16 should be provided with a safe digital environment to foster an appreciation of the risks, thereafter children 16 and above are empowered to make the right choices online.

This research will be relevant to developments that are under way to safeguard children from digital advertising and data collection, at present they do not have sufficient protection in the digital marketplace (*see 7.8*). The study will assist legislators, game developers and those working with privacy policies to understand the interface between data gathering practices and data protection laws within different legal orders in the world. It will also provide guidance to courts (particularly in the EU) in interpreting data protection laws with respect to children as data subjects.

This research will identify gaps in current and prospective data privacy laws with respect to protecting children's digital privacy rights from commercial exploitation.

¹⁴³ Child employment(gov.uk) < <https://www.gov.uk/child-employment>> accessed 23 November 2018.

¹⁴⁴ EU GDPR Article 8.

Recommendations will be made to inform the EU GDPR 2018 in formulating principles that prioritise children's digital rights. By studying the laws that regulate videogame privacy policies, this thesis will inform jurisdictions and companies in drafting laws and policies that will adequately regulate data handling practices of websites and remain commensurate with the reading, understanding and consenting abilities of children.

The original child-friendly model privacy policy will be a step forward towards simplifying data privacy concepts for children and their parents (*Chapter 7*). Videogame websites do not commonly have a separate children's privacy policy. The child-friendly model privacy policy will serve as excellent and essential guidance for videogames to introduce separate child-friendly privacy policies.

The research will also be of interest to parent groups such as Mumsnet (providing online support and advice to parents) in helping them make informed decisions concerning the implications arising from data protection laws and data gathering techniques.

1.5. Primary research questions

This research will:

- a. carry out a comparative legislative analysis of the legislation in the EU, the U.S. and Canada;
- b. carry out a two-part multiple case study of the privacy policies of 10 videogame websites representing the legislation in the EU, the U.S. and Canada;

- c. determine if both industrial practice and data privacy laws remain compatible with the reading, understanding and consenting abilities of children;
- d. formulate an original child-friendly model privacy policy based on observations made and findings concluded from the multiple case study in the thesis.

1.6. Research methodology

A combination of desk-based and empirical research is used as part of the research methodology. Primary and secondary sources are used to consider Directive 95/46/EC, the EU GDPR 2018, the U.S.'s COPPA and Canada's Personal Information Protection and Electronic Documents Act.

A combination of three research methodologies will be adopted to carry out the comparative analysis. First, doctrinal legal research; followed by a functional comparative method; and a multiple case study. The doctrinal legal research in respect of the domestic approaches in selected jurisdiction; a functional comparative method is then applied in relation to these jurisdictions' laws; and a multiple case study considers how these laws are complied with in practice.

The doctrinal legal research will focus on the data privacy rules of the legislation in the EU, the U.S. and Canada. This is followed by functional comparative law analysis that will identify a more specific approach to legal theory incorporating the findings of the legal comparative analysis. Finally, the case study methodology is divided into two parts. The first part will analyse the privacy policies of 10 popular videogame websites.¹⁴⁵ This will determine if privacy policies remain compatible with the

¹⁴⁵ Chapter 5 Part 1 – Online games case studies: Privacy policies and children.

expectation that children should read, understand and consent to its terms. The second part of the study¹⁴⁶ evaluates the same privacy policies and determines if they comply with governing data privacy law. The findings will provide an enriched understanding of whether privacy policies in popular videogames adequately protect children's digital privacy rights both in data handling practices and the governing law. The findings will help the comparative legislative study and make recommendations to make the law adhere to children's digital privacy rights. Finally, mini case studies of three popular children's interactive game sites¹⁴⁷ will be conducted to elicit guidelines for an original child-friendly model privacy policy.¹⁴⁸

1.6.1. Doctrinal legal research

It is concerned with the formulation of legal 'doctrines' through the analysis of legal rules.¹⁴⁹ It is concerned with the discovery and development of legal doctrines and the research question will normally take the form of asking 'what is the law?' This thesis focuses on adequacy of data protection and privacy laws in the EU, the U.S. and Canada (*Chapters 3 & 4*) and then critically evaluates them (*Chapters 5 & 6*).

1.6.2. Functional comparative law analysis

The research will carry out a comparative study of the legislation in the EU, the U.S. and Canada. The comparison will be carried out using Zweigert and Puttfarcken's functional analysis comparative law method.¹⁵⁰ According to Zweigert and

¹⁴⁶ Chapter 6 Part 2 – Online games case studies: Privacy policies and governing data privacy law.

¹⁴⁷ Disney, Harry Potter and BBC CBeebies.

¹⁴⁸ Chapter 7 – Original child-friendly model privacy policy.

¹⁴⁹ P. Chynoweth, 'Legal Research in the Built Environment: A Methodological Framework' (University of Salford, Manchester) <http://usir.salford.ac.uk/12467/1/legal_research.pdf> accessed 3 December 2017.

¹⁵⁰ Konrad Zweigert and Hans-Jurgen Puttfarcken, 'Critical Evaluation in Comparative Law' (1973) 5(4) *Adelaide Law Review* 343, 343–356.

Puttfarcken, different jurisdictions placed on the same footing reveal similarities and dissimilarities between their legislatures, laws and implementation, which can help in finding an ideal solution to a socio-legal problem. The purpose of this study is to identify commonalities and divergences between the EU's, the U.S.'s and Canada's approaches to data protection in the law enforcement sector. The findings of the study will aim to serve as a basis for assessing the need to change laws to safeguard children's data privacy interests. The outcome of the legislative analysis will be applied to the multiple case study of videogame privacy policies to determine if industrial practice remains compatible with governing data privacy laws. This comparison will enable best practices to be identified that can then be used to draft an original child-friendly model privacy policy that aims to be brief, easy to understand and child-friendly. It is hoped that the child-friendly model privacy policy will become a guideline for videogame websites to inform children and their parents about the websites' data handling practices in easy-to-understand, brief and succinct terms.

1.6.3. Case study methodology

The purpose of the study is to carry out a privacy policy content analysis of the selected websites that is accessible to all ages and frequently visited by children. The research has developed criteria for a comparative analysis of the privacy policies of 10 videogame websites, which will emulate the contents of any data privacy law and includes the length of the policy, use of language, placement of the term 'privacy policy' on the webpage, use of tracking technologies etc.

The research uses download statistics and hours of game play to sample online games that are not age-restricted but are nevertheless popular amongst under-18s around the world. For instance, Statista¹⁵¹ presented the most played videogames in November 2015 by share of total time played. Of all-time spent gaming in November 2015, 22.92% was dedicated to playing *League of Legends*. League of Legends was the most played game with 27 million players daily, making it the most played game in the world.¹⁵² The selected games comprise *Candy Crush Saga*, *Pogo*, *Clash of Clans*, *Minecraft*, *Wizards of Warcraft* etc. The researcher chose games from the U.S. and the EU. By studying games from both continents, the study could compare legislative conformity between privacy policies and general game play with native data protection and privacy regimes.

The comparison of data privacy legislation in the multiple videogame case study aims to determine aspects of the law that need to be encouraged and/or strengthened. Best practices from both the legislative analysis and the study of privacy policies have been used in devising an original child-friendly model privacy policy.

1.6.4. Reasons for selection of these methods

Since doctrinal legal research is associated with the discovery and development of legal doctrines (*see footnote 149*), it is associated with the study of legal texts embedded within statutes and case law. The study of data protection and privacy legislation in the EU, the US and Canada can provide a basic understanding of the

¹⁵¹ Statista is a leading statistics company that researches quantitative data, statistics and related information for large corporations and academic institutions. 'About Statista Inc.' (Statista) <<https://www.statista.com/aboutus/>> accessed 21 February 2017.

¹⁵² Ibid, Melody Madhavan, 'How League of Legends Became the Most Popular Game in the World' (*Referral Candy* blog, 6 January 2016) <<https://www.referralcandy.com/blog/league-of-legends-word-of-mouth-marketing/>> accessed 3 December 2017.

underlying principles before a comparative study can be carried out. The functional comparative analysis will compare the three jurisdictions placed on a similar footing, revealing similarities and dissimilarities between them. The study will provide important findings revealing the strengths and weaknesses of each jurisdiction. The doctrinal and functional comparative studies will reveal whether data protection and privacy laws in the EU, the US and Canada adequately protect children's digital privacy rights. The presence of relevant laws is however insufficient, and it is also necessary to consider how these laws are complied with in practice. The multiple case study will determine if data privacy law is complied within practice by carrying out privacy policy content analysis of selected websites. Such an analysis can identify the interface between law and implementation. It can reveal aspects that need encouraging and others that require strengthening. These findings can be used to draft a child-friendly model privacy policy that is easy to read and understand.

1.6.4.1. Rationale for selecting legislatures of the EU, the U.S. and Canada for the comparative legal analysis

This thesis explores the privacy policies of 10 most popular videogame websites in 2015, according to media audience research firms. The thesis evaluates the jurisdictions that govern the data handling practices of the videogame privacy policies. The selected videogames are either governed by the EU or the U.S. law, resulting in the need to study these legislatures. The legislature of Canada is selected because this thesis further develops and updates Canadian lecturer Sara Grimes's

multiple case study of the data privacy issues resulting from data mining¹⁵³ practices in children's videogames.¹⁵⁴ Her study which was conducted more than 10 years ago, primarily looked at End-User License Agreement (EULAs) and data mining practices in children's videogames. This thesis studies privacy policies of children's videogames and the resulting legal issues associated with digital privacy risks. Also, this is a more updated study that looks at data protection and privacy laws that have evolved over time and contemplate the EU GDPR 2018. In addition, legislation in the EU, the U.S. and Canada were selected because these are Western democratic legal systems subject to democratic controls of access and content. Further, the EU, the U.S. and Canada are also some of the largest markets for the online gaming industry (see 5.3.1.1). These legislatures were chosen for the comparative legal analysis even though they have varying constitutional and regulatory scope. Nonetheless, they do settle on similar approaches to data protection and privacy regulation. For instance, verifiable consent¹⁵⁵ is required before the processing of personal data in the EU,¹⁵⁶ the U.S.¹⁵⁷ and Canada¹⁵⁸ in their data privacy laws (see 3.2.5; see 4.3.3.2 & 4.9)

EU academics Milda Macenaite and Eleni Kosta note that the EU GDPR 2018 has been partially inspired by the U.S, COPPA.¹⁵⁹ Therefore, the US experience can inform the debate about the adequacy of EU and Canadian data privacy law over the new data

¹⁵³ Data mining is a process of extraction of useful information and patterns from huge data. It is also called the knowledge discovery process, knowledge mining from data, knowledge extraction or data/pattern analysis. Bharati M. Ramageri, *Data Mining Techniques and Applications* (2010) 1(4) IJCA.

¹⁵⁴ Grace Chung and Sara M. Grimes, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2005) 30(4) *Canadian Journal of Communication*.

¹⁵⁵ The term 'verifiable parental consent' has not been defined by the Data Protection Directive 95/46/EC or the EU GDPR 2018; COPPA Section 6501(9).

¹⁵⁶ Data Protection Directive Article 2(h).

¹⁵⁷ Children's Online Privacy Protection Act 16 CFR 312.5 – Parental consent.

¹⁵⁸ Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) Section 6.1.

¹⁵⁹ Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) *Information & Communications Technology Law* 146.

protection challenges related to children's ability to read, understand and consent to websites' data handling practices. The comparative analysis will provide an opportunity to explore different facets of composite data privacy rules. It will address the wider implications for digital privacy rights of children when playing videogames. Both the EU and the U.S. have varied constitutional and regulatory data privacy law. Legal practitioner, Phil Lee believes that there is a stronger cultural expectation of privacy in the EU than in the US.¹⁶⁰ Currently, the EU and U.S. represent different rules on data protection and the right to privacy.¹⁶¹ The right to privacy in the EU is protected as a fundamental right under the European Union's Charter of Fundamental Rights. In contrast, the word 'privacy' is not even mentioned in the U.S. Constitution. Rather than establishing overarching privacy rules, the U.S. tends to create privacy rights when the need arises for specific regulatory solutions.¹⁶²

While the focus of this thesis is on data privacy legislation in the EU, the U.S. and Canada, there are other major nation states such as Australia, China and Canada that contribute to the videogame industry.¹⁶³ In Australia, the processing of personal data

¹⁶⁰ Phil Lee, 'How Do EU and US Privacy Regimes Compare?' (Fieldfisher, 5 March 2014) <<http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare/>> accessed 10 November 2017; Wojciech Wiewiórowski, 'International Cooperation of Privacy and Data Protection Commissioners' (GIODA, 14 October 2014) <http://www.phaedra-project.eu/wp-content/uploads/2014_10_13_phaedra_mauritius_wiewiorowski-1.pdf> accessed 10 November 2017. This expectation was addressed at the 20th Conference of the International Data Protection Commissioners in Santiago de Compostella, Spain, in 1998, where it was conceded that Europeans lead the U.S. in data protection policies.

¹⁶¹ Cayce Meyers, 'Digital Immortality vs. "The Right to Be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy' [2014] Romanian Journal of Communication and Public Relations <<https://journalofcommunication.ro/index.php/journalofcommunication/article/view/175/177>> accessed 11 November 2017.

¹⁶² *Griswold v Connecticut* 381 U.S. 479 (1965) The Supreme Court struck down a state law that prohibited the sale of contraceptives to married couples, (which affected their right to private and family life) in response to new forms of intrauterine devices that were introduced in the 1960s.

¹⁶³ Jeffrey Hagenmeier, 'Invest In Video Gaming: A Booming Industry In Emerging Markets' (Day Trading Academy, 6 May 2014) <https://webcache.googleusercontent.com/search?q=cache:E2XjWAA5fysJ:https://daytradingacademy.com/invest-video-games-booming-industry-emerging-markets/+&cd=3&hl=en&ct=clnk&gl=uk> accessed 23 January 2018.).

is regulated by the Privacy Act No. 119 of 1988. There are no special data privacy rules for children but consent warrants capacity. To determine if an individual under 18 years has capacity to provide consent, website operators will refer to the age, mental or physical disability, and limited understanding of English¹⁶⁴ In China, rules and regulations relating to informational privacy were introduced in the form of the Cybersecurity Law, on 1 June 2017 but it does not deal with children's digital privacy rights.¹⁶⁵

In India, the Information Technology Act 2000 (No. 21 of 2000) regulates data processing but it does not provide specific provisions for children's digital privacy rights. Since these jurisdictions did not provide specific laws for children's data protection and privacy rights and China's data privacy law is presented in a different language, they were not selected for the comparative law study

1.6.4.2. Data Protection Directive 95/46/EC – Now repealed

European laws privilege the rights of individuals to control the dissemination of information about them. Data storage and periods of retention in EU were earlier regulated by the EU's Directive 95/46/EC,¹⁶⁶ which served to protect the processing of the personal data of European citizens. The Directive determined how personal

¹⁶⁴ Australian Privacy Principles (APP) Chapter B.53 (Australian Government)
<<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#consent>>
accessed 23 January 2018.

¹⁶⁵ 'Overview of China's Cybersecurity Law' (KPMG)
<<https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>>
accessed 23 January 2018; 'Emerging Trends in Paint India Gaming Industry'
<[https://www.techsciresearch.com/admin/gall_content/2017/6/2017_6\\$thumbimg114_Jun_2017_074442683.pdf](https://www.techsciresearch.com/admin/gall_content/2017/6/2017_6$thumbimg114_Jun_2017_074442683.pdf)>
accessed 23 January 2018.

¹⁶⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

data will be gathered, maintained, updated, stored, protected and disposed of.¹⁶⁷ According to Rosario Imperiali, Directive 95/46/EC needed modernising¹⁶⁸ to address privacy concerns raised by technological advancements in social networking sites, cloud computing services etc. It did not address children as data subjects and left legal uncertainty regarding profiling and data retention terms.¹⁶⁹ Accordingly, the European Commission proposed the EU GDPR 2018,¹⁷⁰ which modernises data protection laws and offers special measures for children. It specifically incorporates the practice of ‘profiling’.¹⁷¹ Both the Directive 95/46/EC and EU GDPR 2018 need critical and detailed analysis, to determine whether children are adequately protected online. This is largely carried out in *Chapter 3*.

1.6.4.3. The Canadian data privacy regime

This thesis considers the data protection and privacy laws in Canada (*see 4.9*). Canadian legal practitioner Karen Levin believed that Canada was at the forefront of privacy protection, and that the protection of personal data was regulated without specific regard for children.¹⁷² According to Colin J. Bennett et al., in 2014, Canada’s Personal Information Protection and Electronic Documents Act (‘PIPEDA’) is considered a beacon when compared with the data privacy regimes of other

¹⁶⁷ Mathieu Gorge, ‘The implications for storage of EU data protection regulation’ (ComputerWeekly.com) <<http://www.computerweekly.com/feature/The-implications-for-storage-of-EU-data-protection-regulation>> accessed 28 December 2016.

¹⁶⁸ Rosario Imperiali, ‘The Data Protection Compliance Program’ (2012) 7(3) *Journal of International Commercial Law and Technology* 285, 285–288.

¹⁶⁹ DLA Piper, ‘EU Study on the Legal Analysis of a Single Market for the Information Society’ (Europa, November 2009) <www.europa.eu> accessed 28 December 2016.

¹⁷⁰ Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) 2012.

¹⁷¹ EU GDPR 2018 Article 22.

¹⁷² Karen Levin, ‘A Look at the Protection of Children’s Personal Information in an Online Context’ (Lexology, 3 November 2011) <<https://www.lexology.com/library/detail.aspx?g=9decc24d-ac5f-4bbf-b8cc-6b9710523480>> accessed 10 November 2017.

countries.¹⁷³ Its enactment was motivated by Directive 95/46/EC and the European Commission decided that it provides adequate protection to data transferred from EU to Canada.¹⁷⁴

The fact that PIPEDA was approved by the EU provided the impetus to include it in the jurisdictional comparative analysis. Questions arose about whether the U.S. – EU Safe Harbour Framework¹⁷⁵ decision impacted the PIPEDA (*see 5.5.3 & 5.5.4*). Since Safe Harbour only applied to data that was transferred from the EU to the US, PIPEDA was not directly affected.¹⁷⁶ However, Canadian organisations could be transferring or storing EU citizens' data to or within the territory of the U.S. If this happens, Canada will have to find alternative means that offer adequate levels of protection to EU citizens' data.

A popular videogame website governed by Canadian data privacy law could not be identified (*see 5.3.1.3*). Princess Isabella (selected for the multiple case study to be carried out in Chapter 5) was developed by Canadian developer Gogii Games¹⁷⁷ but it is owned by Big Fish Games and governed by the laws of the state of Washington, U.S.A. (*Chapter 5 Table 5*). Therefore, the comparative functional analysis will

¹⁷³ Colin J. Bennett and others, *Transparent Lives: Surveillance in Canada* (AU Press 2014).

¹⁷⁴ European Commission, 'Data Protection: Commission Recognises Adequacy of Canadian Regime' (Europa, 14 January 2002) <http://europa.eu/rapid/press-release_IP-02-46_en.htm?locale=en> accessed 15 November 2017.

¹⁷⁵ The U.S.–EU Safe Harbour Framework was a system of rules that had to be complied with by US-based organisations when data from EU was transferred to the US, so as to comply with the data protection principles of the Data Protection Directive 95/46/EC. Ernst-Oliver Wilhelm, 'A Brief History of Safe Harbour' (iapp) <<https://webcache.googleusercontent.com/search?q=cache:tVy-pO98WA4J:https://iapp.org/resources/article/a-brief-history-of-safe-harbor/+&cd=7&hl=en&ct=clnk&gl=uk>> accessed 15 March 2018.

¹⁷⁶ 'Is Canada Safe from the Safe Harbour Decision?' (Lexology, 13 December 2015) <<https://www.lexology.com/library/detail.aspx?g=cf0e7076-8930-4b74-9493-ca5522c8e5b2>> accessed 15 November 2017.

¹⁷⁷ *Princess Isabella: A Witch's Curse* <<https://www.giantbomb.com/princess-isabella-a-witches-curse/3030-46348/>> accessed 15 November 2017.

principally consider the EU and U.S. data privacy laws that regulate the data handling practices of websites.

1.6.4.4. The U.S. data privacy regime

The U.S. does not have a parallel equivalent to the EU data privacy regime. The data privacy rules deal with specific issues from federal rules that deal with children's online privacy¹⁷⁸ to state-specific rules¹⁷⁹ that apply to any website company or person that collects personally identifiable information from Californian users. The U.S. provides specific rules on treating children as a special class of data subjects. There are rules on the age at which children can provide online consent; as well as rules that dictate the conduct of privacy notices from their placement to how distinguishable they should be (*see 4.4.1 & 4.5; 6.2.1*).

The varying regulatory approach creates challenging problems for companies that must follow different data privacy standards and the need to protect children's data privacy when it is transferred across borders. It is important for corporations as well as data users to know about their responsibilities and the level of protection offered by the countries, the data is transferred to.

This thesis provides a useful insight into the legal protection accorded to online privacy rights of videogame website users. Since videogame websites attract a large younger audience, the analysis will determine the adequacy of legal protections offered to the privacy of children's digital personal data. The U.S. has gone a step

¹⁷⁸ Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505.

¹⁷⁹ California Online Privacy Protection Act 2003– California Business and Professions Code sections 22575–22579.

further and enacted the COPPA,¹⁸⁰ which specifically relates to protecting children’s personal data. Directive 95/46/EC did not provide special protection for children. This position changed with the EU GDPR 2018, which treats children as a special class of data subjects.¹⁸¹ According to Paul Schwartz, a generation of comparative law scholars have demonstrated that no legal system exists free from the influence of others.¹⁸² The EU data privacy law is in a state of transition and both legislatures can learn from each other’s principles and adopt data privacy laws that protect the online privacy rights of children.

Key themes of the thesis

This study is limited to three key themes in this study: (1) the varying ages for consent used in different jurisdictions; (2) the issue with reliability of online consent methods; and (3) the difficulty with the readability of privacy policies. This combination of research methodologies will build a comprehensive understanding of the adequacy of data privacy laws in protecting children’s digital privacy. Additionally, it will also reveal if data privacy laws are complied with in practice.

Different jurisdictions have varying ages for online consent (*see 4.10.1*). This can create difficulties because a 14-year-old child in Germany (where the age of consent is 14 years) will be treated a child data subject but an adult data subject in the UK (where the age of consent is 13 years). Jurisdictions will benefit from a common age

¹⁸⁰ Children’s Online Privacy Protection Act, 15 U.S.C. §§6501–6506.

¹⁸¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications).

¹⁸² Paul Schwartz, Comparative Contractual Privacy Law: The U.S. and EU <https://www.law.uchicago.edu/files/file/schwartz_comparative_contractual_privacy_law.pdf> accessed 15 November 2017.

for consent to remove this uncertainty. The United Nations Convention on the Rights of a Child ('UNCRC') defines a child as anyone under the age of 18 years (*see footnote 610*) but allows jurisdictions to take account of cultural variations. There are a variety of approaches towards choice of age for consent.¹⁸³ In England children can give legal consent to sex at the age of 16 under the Sexual Offences Act 2003; children aged 13 years are entitled to work part-time;¹⁸⁴ the minimum age for driving a car is 17 years¹⁸⁵ (*see section 1.4*) This thesis proposes maximum protection by capturing widest range of childhood owing to the various online digital privacy risks children are exposed to. In keeping with the recommendations of the EU GDPR, parental consent should be required from children under 16 years of age (*see 4.10.1*). There are strong arguments for introducing tools to empower children who can then protect themselves from digital risks.¹⁸⁶ It is also contended that for children to have awareness of digital privacy risks, they need to experience a secure and safe digital environment. The internet presents greater risks, and children need additional protection.¹⁸⁷ For practical purposes, this thesis proposes that children be defined as anyone under the age of 18 years.

The concept of consent is one of several legitimate basis for allowing personal data processing.¹⁸⁸ The Directive 95/46/EC explained consent as 'any freely given specific and informed indication of his wishes by which the data subject signifies his

¹⁸³ Section 8 (1) of the Family Law Reform Act 1969.

¹⁸⁴ Child employment(gov.uk) < <https://www.gov.uk/child-employment>> accessed 23 November 2018.

¹⁸⁵ The Motor Vehicles (Driving Licences) Regulations 1999 section 9.

¹⁸⁶ Dawn Watkins and others, Exploring Children's Understanding of Law in Their Everyday Lives (2018) 38(1) Legal Studies; 'Assessing Children's Understanding of Law through Digital Gaming' (University of Leicester, 4 July 2014) <<https://www2.le.ac.uk/departments/law/news-events/law-news/assessing-children2019s-understanding-of-law-through-digital-gaming>> accessed 23 November 2018.

¹⁸⁷ EU GDPR Recital 38 and 75.

¹⁸⁸ EU GDPR Article 6(1)(a).

agreement to personal data relating to him being processed'.¹⁸⁹ The EU GDPR added the additional element that the data subject should provide consent by way of a written declaration.¹⁹⁰ Digital consent is difficult to prove as it is impossible to confirm the identity of the person giving consent. The requirement of parental consent mechanisms can easily be surpassed by children providing false ages or fictitious email addresses. This thesis proposes that when processing children's personal data, website operators should rely on other data protection principles of transparency and fairness rather than depend on consent (*see footnotes 113-115;680-682*)

The third main theme in this study is the difficulty in reading privacy policies. The multiple case study revealed that privacy policies are difficult to access; they are lengthy, complicated documents and not child-friendly (*see Chapter 5*). This thesis proposes that amongst other things website operators should employ the Flesch reading score (see 5.5.2.3.) This means that privacy policies should easily be read by children under 13 years of age. According to this thesis, children under 16 years are not required to read privacy policies owing to their parents giving consent. But a lower age limit and the ease of readability will encourage parents/legal guardians and children aged 16-18 years to read privacy policies.

1.7. Overview and structure of the thesis

This thesis aims to deliver a model for simplified child-friendly digital privacy policies. Typical videogame privacy policies are long and tedious to read, containing technical and legal jargon which deters children from reading them. Children are therefore

¹⁸⁹ Directive 95/46/EC Article 2(h).

¹⁹⁰ EU GDPR Article 4(11).

more at risk of sophisticated data tracking technologies and consequences of data breach. This research contributes to literature with a view to improving industrial practices in treating children as a special class of data subjects.

This study comprises eight chapters. This first chapter has introduced the rationale for this thesis: the underlying problem relating to children's digital privacy rights when playing videogames, a literature review of the academic works identifying a gap, the research questions and the methodology adopted to conduct the research.

Chapter 2 explains the right to data protection and privacy by listing the preliminary legislative attempts to codify the normative value of data protection and the right to privacy into fundamental law. The chapter will also consider the discord between theorists about whether the two rights are separate or overlapping in nature.

Chapter 3 critically analyses the main principles of the data protection and privacy regimes operating in the EU. It will look at Directive 95/46/EC which was the main data privacy law in the EU until 25th May 2018. It will also evaluate the principles of EU GDPR 2018, which replaced Directive 95/46/EC on 25th May 2018.

Chapter 4 critically analyses the main data protection and privacy laws in the U.S. and Canada. In the U.S., COPPA applies to websites directed to children. However, federal states have established their own data privacy laws and therefore the chapter also considers such laws that govern the privacy policies of the videogame websites selected for this study.

Chapter 5 carries out a multiple case study of 10 videogame website privacy policies selected from the legislation in the EU, the U.S. and Canada. The study looks at the

content of privacy policies and analyse whether they comply with expectations for children to read, comprehend and consent to such terms.

Chapter 6 evaluates the data protection and privacy legislation that currently regulates the privacy policies of the videogame websites in line with the mental maturity and reading abilities of children.

Chapter 7 compiles the findings of Chapters 5 and 6 to produce a child-friendly model privacy policy based on best practices that is concise and easy to read and understand. The original child-friendly model privacy policy aims to alter the current practice of lengthy, technical and difficult-to-read privacy policies aimed at children as young as 13 years of age.

Chapter 8 presents the conclusions, which draw on the analysis of the previous chapters. It restates the principal findings, the importance of the findings in the academic field of children's digital privacy rights with respect to videogame websites and an explanation of how the research questions were answered by the methods employed to conduct the study and the evidence found.

The next chapter evaluates the earliest attempts to codify data protection and privacy with respect to children. It explains the importance of the right in the current cyberworld and jurists' understandings of whether data protection law and right to privacy are separate or disparate rights with overlapping features.

The law studied in this thesis is stated as at 30th June 2018.

CHAPTER TWO

UNDERSTANDING THE CONCEPTS OF PRIVACY AND DATA PROTECTION

2.1. Introduction

This chapter examines the initial legislative attempts to codify the right to privacy and data protection. It explains the importance of the two rights in the current cyberworld with respect to children and examine whether the two rights are separate or overlapping in nature. The discussion lays down a concrete understanding of data protection and privacy, which then underpins the legislative analysis in subsequent chapters of this thesis.¹⁹¹

In this chapter, the first section defines right to privacy, the preliminary international legislative attempts in the selected legislatures to codify it, and its importance in the rapidly burgeoning cyberworld. Digital privacy will be asserted through recent privacy breaches in the videogame industry. There will be a review of the digital privacy awareness of parents and children followed by the legislative attempts to codify right to data protection and privacy. Both data protection and right to privacy are different rights with interlocking features, which are premised on the concept that individuals have a right to privacy over their information. Finally, this notion of the two separate rights will be considered, with a concluding paragraph at the end of the chapter.

¹⁹¹ Chapter 3 – The current European digital privacy legislation; Chapter 4 – Data protection and privacy framework in the U.S. and Canada.

2.2. Definition of privacy

Privacy is a universal concept adhered to differently between societies.¹⁹² Thomas M. Cooley was one of the earliest jurists to define privacy 'as the right to be left alone'.¹⁹³ German philosopher Jürgen Habermas emphasised the importance of a private sphere needed to protect essential parts of our lives from the glare of ruling powers.¹⁹⁴ Theorists like Judith Thomson found privacy as a cluster of derivative rights where an individual's private interest can be protected through the operation of other rights including the right to security and property.¹⁹⁵ Miller has therefore stated that privacy is 'difficult to define because it is exasperatingly vague and evanescent'.¹⁹⁶

The rights of children include a wide assortment of civil, political, economic, social and cultural rights. There are two general types of children's rights: to treat children as autonomous persons under the law and to place an obligation on society to protect children because of their dependency.¹⁹⁷ As society became increasingly aware of the growing social inequalities, privacy aspects developed around children and family law.¹⁹⁸ A review of the periodic literature shows a wide spectrum of children's privacy

¹⁹² James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 Yale Law Journal 1151; Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193.

¹⁹³ Colin J. Bennett, *Regulating Privacy* (Cornell University Press 1992); Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008); Monroe E. Price, Stefaan Verhulst and Libby Morgan, *Routledge Handbook of Media Law* (Routledge 2013).

¹⁹⁴ Jürgen Habermas, *The Structural Transformation of the Public Sphere* (MIT Press 1991).

¹⁹⁵ Andrei Marmor, 'What Is the Right to Privacy' (2015) 43(1) Philosophy and Public Affairs 3 <<http://onlinelibrary.wiley.com/doi/10.1111/papa.12040/full>> accessed 21 November 2015; Anita A. Allen, 'Uneasy Access: Privacy for Women in a Free Society' (1992) 101(3) The Philosophical Review <<http://doi.org/10.2307/2186088>> accessed 23 November 2015.

¹⁹⁶ Arthur Miller, *The Assault on Privacy: Computers, Databanks and Dossiers* (University of Michigan Press 1971).

¹⁹⁷ Munyaradzi Mawere, *The Political Economy of Poverty, Vulnerability and Disaster Risk Management* (Langa RPCIG 2018).

¹⁹⁸ Sara S. Klein, 'Right to Privacy and Children's Rights/Family Law: A Selective Bibliography' [1994] Journal Articles. Paper 1152.

rights. These include privacy and education, which could concern the teacher–student interface¹⁹⁹ and sex education in schools. Children’s right to privacy also included parental consent, which was required by minors for abortions.²⁰⁰

The rich debate on privacy between legal scholars, philanthropists and politicians²⁰¹ is so broad, it is virtually impossible to codify in universally acceptable terms. Owing to the limitation of this chapter, focus will be placed on the interrelationship between data protection and right to privacy in the specific context of protections and legal development in the digital environment. This chapter considers the extent to which privacy has helped formulate data protection law.

2.2.1. Privacy codified in international legislative Instruments

In the EU, one of the most prominent international attempts to recognise privacy rights is the European Convention on Human Rights 1950 (‘ECHR’).

2.2.2. European Convention on Human Rights 1950

The ECHR is an international treaty that protects human rights and fundamental freedoms in all state signatories.²⁰² In Article 8 it protects the right to respect for

¹⁹⁹ Mary Gordon Baker, ‘The Teacher’s Need to Know versus the Student’s Right to Privacy’ <https://webcache.googleusercontent.com/search?q=cache:jKEQKYMJnOAJ:https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015-sac/gordon_baker_mary.pdf+&cd=2&hl=en&ct=clnk&gl=uk> accessed 8 February 2018.

²⁰⁰ *Planned Parenthood v Danforth*, 428 US 52 (1976); the right to privacy also concerned access to contraception in general, as well as in educational settings. Sara S. Klein, ‘Right to Privacy and Children’s Rights/Family Law: A Selective Bibliography’ [1994] Journal Articles. Paper 1152.

²⁰¹ Edward Keynes, *Liberty, Property and Privacy* (Penn State Press 1996).

²⁰² European Convention on Human Rights (Council of Europe, 1950) <https://www.echr.coe.int/Documents/Convention_ENG.pdf> accessed 24 March 2016.

private and family life, home and correspondence,²⁰³ which is subject to proportionate and lawful restrictions.²⁰⁴

The European Court of Human Rights ('ECtHR') gave two important decisions in relation to the liability of online user-generated content and implications of the freedom of expression for a business running a website.²⁰⁵ In the *Magyar* case,²⁰⁶ the ECtHR held that an online news portal was not liable for offensive comments posted by readers on its website. The court cited the earlier controversial judgment given by the Grand Chamber in the *Delfi* case,²⁰⁷ which established the liability of the online news portal because the comments were not only offensive but amounted to unlawful hate speech causing incitement to violence.

The court's approach to interpret the ECHR autonomously²⁰⁸ has resulted in many elements within the right to privacy including family law, property law and secret surveillance. At present and for the purposes of this thesis, the discernment of privacy in online surveillance mechanisms will be looked at in considerable detail. The following table lists the attempts in the pre-digital environment to codify privacy law.

²⁰³ European Convention on Human Rights 1950, Article 8(1); Article 8 right to a private and family life (Liberty) <<https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-8-right-private-and-family-life>> accessed 24 March 2016 ; David Harris and others, *Law of the European Convention on Human Rights* (Oxford University Press 2009).

²⁰⁴ European Convention on Human Rights 1950, Article 8(2); *Handyside v the United Kingdom* (5493/72) [1976] ECHR 5 [48], [49]; European Convention on Human Rights 1950, Article 10; Steven Greer, 'The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights' (Council of Europe, 2000) <[http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17\(2000\).pdf](http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf)> accessed 30 March 2016.

²⁰⁵ *Grand Chamber Case of Delfi AS v Estonia* (Application no. 64569/09) 16 June 2015.

²⁰⁶ *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (Application no. 22947/13) 2 February 2016.

²⁰⁷ *Delfi AS v Estonia* (Application no. 64569/09) 16 June 2015.

²⁰⁸ *Gaskin v United Kingdom* (1989) 12 EHRR 36; *Campbell v UK* A 233 (1992); 15 EHRR 137 [32]; Ursula Kilkelly, 'A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (Council of Europe) <[http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01\(2003\).pdf](http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01(2003).pdf)> accessed 30 March 2016.

Table 1 Codification of privacy law in the pre-digital environment

Legislation	Year of promulgation
The Universal Declaration of Human Rights	1948
European Convention on Human Rights	1950
International Covenant on Civil and Political Rights ²⁰⁹	1966

2.2.3. The Universal Declaration of Human Rights 1948

The Universal Declaration of Human Rights 1948 ('UDHR') was a milestone document in the history of human rights. Article 12 prevents anyone from being subjected to arbitrary interference with their privacy, family, home, correspondence, honour and reputation.²¹⁰ Later, these same words resonated in Article 17 of the International Covenant on Civil and Political Rights 1966, with the right to the protection of law against interference encoded separately in Article 17(2).

Although these instruments create obligations for the state to protect individuals' privacy, they can impact on children's privacy rights. The UDHR does not expressly recognise children's rights but Article 25, the standard of living provision, codifies that children are entitled to 'special care and assistance'.²¹¹ The UDHR places obligations on the state and parents to uphold the rights of children and paved the way for the

²⁰⁹ UN General Assembly, International Covenant on Civil and Political Rights (United Nations, 16 December 1966) <<http://www.refworld.org/docid/3ae6b3aa0.html>> accessed 9 May 2017.

²¹⁰ The Universal Declaration of Human Rights 1948, Article 12.

²¹¹ Gordon Brown, *The Universal Declaration of Human Rights in the 21st Century: A Living Document in a Changing World* (openbookpublishers 2016).

United Nations Convention on the Rights of the Child ('UNCRC'),²¹² which articulated specific rights for children.

2.2.4. The United Nations Convention on the Rights of the Child

Protecting children's rights is primarily the responsibility of the parent or legal guardian. Sometimes, the parent can falter in providing the required protection. According to Sonia Livingstone and Amanda Third, the UNCRC was formulated to ensure that states would protect children's rights whenever needed.²¹³ The four guiding principles of the UNCRC relating to digital environments are children's right to life, survival and development,²¹⁴ to have their best interests respected,²¹⁵ to non-discrimination²¹⁶ and to be heard.²¹⁷ In 1996, the Committee on the Rights of Child recognised the interrelation between children, media and the promotion of the UN CRC on child participation and integrity of the child.²¹⁸

²¹² UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3 <<http://www.refworld.org/docid/3ae6b38f0.html>> accessed 4 November 2017.

²¹³ Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (SAGE journals, 10 May 2017) <<http://journals.sagepub.com/doi/full/10.1177/1461444816686318>> accessed 9 February 2018. States are required to help families protect children's rights and create an environment where they can grow and reach their potential; UNCRC Article 4.

²¹⁴ UNCRC Article 6.

²¹⁵ UNCRC Article 3.

²¹⁶ UNCRC Article 2.

²¹⁷ UNCRC Article 12.

²¹⁸ A working group was established that focused on child participation in the media and better implementation of the Convention. Amanda Third et al. 'Children's Rights in the Digital Age' (UNICEF) <https://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf> accessed 9 February 2018.

More importantly, the Convention defines anyone below the age of 18 as a child.²¹⁹ This is relevant because, presently, legislatures have inconsistent provisions on the age at which children can give online consent,²²⁰ leading to confusion on children's applicable data privacy law. Videogame websites may be registered in one country and accessed in another, and a child user can be treated as a child in one jurisdiction and an adult in the other. For these reasons, this thesis recommends that legislatures should define a child as anyone under the age of 18 years, which is compatible with the definition of child under the UNCRC.

2.3. Rights of children in the EU

The fundamental rights of individuals in EU were created in different documents and at other times.²²¹ In December 2000 the EU decided to include all these rights in a single document known as the Charter of Fundamental Rights of the European Union ('EUCFR'). Article 24 of the EUCFR provides that 'Children shall have the right to such protection and care as is necessary for their wellbeing'. The same article specifies further on that 'In all actions relating to children ... the child's best interests must be a primary consideration'. On this basis, authorities including EU countries are obliged to give primary consideration to the child's best interest in the exercise of competence and implementing EU law.

²¹⁹ UNCRC Article 1.

²²⁰ In Germany, the age of consent is 14 years. Carlo Piltz, 'The European Data Protection Law and Minors – No Legal Certainty' (German IT Law, 2014) <<http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty/>> accessed 12 January. In UK, the age of consent is 16 years. Ibid. In the U.S., the Children's Online Privacy Protection Act protects the digital privacy of children under 13 years of age. Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505; 16 CFR §312.2.

²²¹ 'Q&A: Charter of Fundamental Rights' (BBC, 2007) <<http://news.bbc.co.uk/1/hi/world/europe/6225580.stm>> accessed 31 March 2016.

The Treaty of Lisbon is a crucial step that introduces obligations on the EU in developing an effective legislative strategy for protecting children's rights. Article 3(3) of the Treaty on European Union provides that '[t]he Union shall combat social exclusion and ... and protection of the rights of the child'.

Data protection and privacy law was introduced in EU with the now repealed Data Protection Directive 95/46/EC²²² and the Treaty on the Functioning of the European Union,²²³ which will be considered further below.

2.3.1. Children Act 2004 (UK)

Countries have introduced their own state-specific laws to bring children's welfare under statutory authority. The Children Act 2004²²⁴ was created to better regulate official intervention in the interests of children in the UK. The Act created the Office of the Children's Commissioner,²²⁵ which has enabled risks of the digital environment to be identified. Anne Longfield, children's commissioner for England, published a report titled 'Growing Up Digital'²²⁶, stating that children are signing up to social media sites and end up giving away personal data and exposing themselves to online grooming, abuse etc (*see footnote 46*). She proposed a digital citizenship programme, which would be compulsory in every school from the age of four to 14 years and would focus on 'digital resilience'.²²⁷ The report attracted several recommendations

²²² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

²²³ Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union – Consolidated version of the Treaty on the Functioning of the European Union – Protocols – Annexes – Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 – Tables of equivalences.

²²⁴ Children Act 2004 Chapter 31.

²²⁵ Children Act 2004 Part 1.

²²⁶ Children's Commissioner, 'Growing Up digital' (The Children's Commissioner's Office)

<<https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/>> accessed 18 November 2018.

²²⁷ Ibid.

to improve children's digital experience. The Department for Digital, Culture, Media and Sport (DCMS) published the 'Internet Safety Strategy' Green Paper, which commits to carrying out a consultation on a school curriculum that will meet the needs of internet and social challenges.²²⁸

The next section will consider the relationship between the right to privacy and the internet. It will look at the reasons why privacy should matter when children are using the internet. It will consider renowned recent cases of videogame website data breaches and both parents' and children's awareness of digital risks.

2.4. Importance of privacy in the cyber world

The importance of privacy in the rapidly burgeoning cyberworld cannot be emphasised enough.²²⁹ The technological revolution has brought immense benefits to computer users, but it has also facilitated criminal activities such as identity theft, stolen/lost data, hacking, cyber-trolling, bullying, harassment etc.²³⁰

In the digital realm, we manufacture a virtual personification of ourselves, engaging in personal affairs from sharing pictures to conducting online banking and much more. In the real world, we place our hand on top of the keypad as a shield when inputting the PIN (personal identification number) into a through-the-wall ATM (automatic teller machine)²³¹ but we may not be so conscious in the digital

²²⁸ Anne Longfield, 'Growing Digital One Year On' (The Children's Commissioner's Office, 6 February 2018) <<https://www.childrenscommissioner.gov.uk/2018/02/06/growing-up-digital-one-year-on/>> accessed 24 February 2018.

²²⁹ General Assembly, 'Resolution 68/167 The Right to Privacy in the Digital Age' (United Nations, 2014) <<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>> accessed 25 March 2016.

²³⁰ Mythili Raman, 'Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime' (Department of Justice) <<http://www.justice.gov/iso/opa/ola/witness/02-04-14-cmr-raman-testimony-re-privacy-in-the-digital-age-preventing-data-breac.201427115.pdf>> accessed 25 March 2016.

²³¹ '7 Ways to Stay Safe when Using ATMs' (moneyways.co.uk, 2015) <<http://moneyfacts.co.uk/guides/credit-cards/7-ways-to-stay-safe-when-using-atms/>> accessed 25 March 2016.

environment. So why should our views on privacy of data submitted online be any different? Databases can be accessed through computers that are usually networked, via the internet, risking an element of misuse and unauthorised access to the information. Individuals' digital data can be subjected to two different kinds of threats: identity theft or identity fraud and misapplication, mishandling or misprocessing of data.²³² This can entail security risks including commercial exploitation, which increases the chances of harm and the misuse of children's personal data.²³³

Online users can be subjected to multiple forms of privacy risks when they use the internet.²³⁴ For the purpose of this thesis, the focus will be on the possible digital privacy risks after the submission of personal information when users are prompted by websites they visit.

2.4.1. Digital privacy risks resulting from data tracking practices

Rapid technological changes, the quick development of the internet, electronic commerce and sophisticated methods of collecting, analysing and using personal information have made digital privacy a grave concern today.²³⁵

²³² Andrew Murray, *Information Technology Law: The Law and the Society* (2nd edn, OUP).

²³³ Chapter 1 Section 1.1; Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) *Information & Communications Technology Law* 146. Storing large quantities of data make it susceptible to data hacking and breaches. A child's personal information hack can leave them vulnerable as the data can be disclosed to third parties or sold on black markets. Children can be subject to risks of identity theft loss of reputation/confidence and discrimination. Sonia Livingstone and others, 'Risks and Safety on the Internet' (The London School of Economics and Political Science) www.eukidsonline.net accessed 4 November 2017.

²³⁴ Sonia Livingstone and others, 'Risks and Safety on the Internet' (The London School of Economics and Political Science) <www.eukidsonline.net> accessed 4 November 2017.

²³⁵ Dileep Kumar Singh and Vishnu Swaroop, 'Data Security and Privacy in Data Mining: Research Issues & Preparation' (2013) 41(2) *IJCTT* 194.

People and especially children are extensive online users. They carry out a host of activities, which include but are not limited to using social media, search engines and playing online games. A plethora of gaming devices are at the disposal of children including gaming consoles and handheld devices such as the Sony PlayStation, the Sony PSP, the Xbox, the Wii and the Nintendo 3DS.²³⁶ The internet has become very easily accessible and operable to individuals of all ages. According to the 'Connected Kids Report', children between the ages of five and 16 are spending up to 6.5 hours a day in front of a TV, games console, mobile phone, computer or tablet.²³⁷ Children may submit personal information to register with the website. The information is collected, stored with the host website and shared across vast spans of commercial interests.

One of the most probable risks to privacy is in the form of data breaches. The online community has been plagued by privacy breaches because the IT infrastructure is not robust.²³⁸ Such unexpected leaks could result in the exposure of millions of customers' personal data, from their names and addresses to their social security numbers and health, bank and other financial details.²³⁹ This has concerned parents about the safety of their children's personal data. A survey conducted by ESET²⁴⁰ revealed that 71% of parents have security concerns about their children sharing

²³⁶ Ibid 100–101.

²³⁷ Childwise is a market research firm that compiled the 'Connected Kids Report' forming a framework of children's media habits from 1995 till 2015. 'New Report Predicts Future Technology Trends among Children and Young People' (Childwise, 2015) <<http://www.childwise.co.uk/reports.html>> accessed 27 November 2015.

²³⁸ Sudhakar Sathiyamurthi, 'The Struggle for Privacy and the Survival of the Secured in the IT Ecosystem' (ISACA, 2011) <<http://www.isaca.org/Journal/archives/2011/Volume-2/Pages/The-Struggle-for-Privacy-and-the-Survival-of-the-Secured-in-the-IT-Ecosystem.aspx>> accessed 25 March 2016.

²³⁹ Carolyn Duffy Marsan, '15 Worst Internet Privacy Scandals of All Time' (networkworld, 26 January 2012) <<http://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html>> accessed 18 November 2015.

²⁴⁰ ESET (Enjoy Safer Technology) supplies products for the comprehensive protection of everyday online activities in private homes and businesses <<https://www.eset.com/int/>> accessed 10 February 2018.

personal information with third parties.²⁴¹ Children may recklessly or unknowingly give personal information to third parties about themselves and their parents/legal guardians.²⁴² A survey carried out by VoucherCodes.co.uk revealed a startling discovery that a fifth of children know how to use their parents' credit card details to buy things online.²⁴³

2.4.2. Literature review: privacy breaches in videogame websites

Parents are rightly concerned about the safety of their children's personal data. According to the Identity Theft Resource Center, 5,754 data breaches were recorded between November 2005 and November 2015, with 783 breaches occurring in 2014.²⁴⁴

As technology develops, data breaches have become very common.²⁴⁵ In the first half of 2017, data records compromised numbered 1,901,866,611.²⁴⁶

²⁴¹ '88% of Parents Concerned about What Children Can Access Online, Reveals Survey' (ESET) <<https://webcache.googleusercontent.com/search?q=cache:sgpFj98w6B0J:https://www.eset.com/int/about/newsroom/press-releases/announcements/88-of-parents-concerned-about-what-children-can-access-online-reveals-survey/+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 10 February 2018.

²⁴² Anita Allen, *Unpopular Privacy: What Must We Hide* (Oxford University Press 2011).

²⁴³ Erica Sandberg, 'More Parents Giving Their Kids Credit Cards' (creditcards.com, 23 June 2017) <<https://webcache.googleusercontent.com/search?q=cache:BsM0l-WhREEJ:https://www.creditcards.com/credit-card-news/more-parents-giving-kids-credit-cards.php+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 24 February 2018.

²⁴⁴ Lauren Sporck, 'The 8 Worst Data Breaches of All Time' (Network security, 2016) <<http://www.networkcomputing.com/net-security/8-worst-data-breaches-all-time/23644893>> accessed 25 March 2016.

²⁴⁵ In 2007, the TJX chain, which includes Marshalls and TJ Maxx, found that 45.7 million customers' credit and debit card numbers were stolen over a period of 18 months. 'T.J. Maxx Theft Believed Largest Hack Ever' (Nbcnews.com, 2007) <http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever/> accessed 29 March 2016.

²⁴⁶ <<https://breachlevelindex.com/>>. It can occur in almost any industry and hackers keep using sophisticated means to steal customer data. When Talk Talk was hacked, loss of confidential customer data resulted in losses worth millions. Kamal Ahmed, 'Talk Talk Hack Cost upto £35 m' (BBC News, 11 November 2015) <<http://webcache.googleusercontent.com/search?q=cache:QyVbhKWW5nwJ:www.bbc.co.uk/news/uk-34784980+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 18 November 2015.

Fashion Fantasy Game is an online game that allows users to design and sell virtual fashion items.²⁴⁷ The game had more than 2.5 million members in 2017.²⁴⁸ It does not provide an age rating, but the privacy policy discusses registration requirements for children under 13 years of age under the heading 'Special Note to Children'. In 2016, information belonging to users both past and present was stolen by cybercriminals.²⁴⁹ Troy Hunt, operator of breach notification firm 'Have I Been Pwned', writes that the breach initially went unnoticed by *Fashion Fantasy Game*, resulting in millions of user account credentials being leaked online.²⁵⁰ Even more disconcerting is the fact that *Fashion Fantasy Game* has not acknowledged any kind of data breach on the firm's website or social media channels.

Gamigo is a massively multiplayer online-role playing game (MMORPG),²⁵¹ serving a North American and European audience.²⁵² In 2012, there was a server breach that resulted in 8,243,809 user account credentials including email addresses and encrypted passwords compromised and leaked online.²⁵³ Although the website informed users about the breach and requested them to change their passwords, it would bring little comfort to users whose information was available on all spam lists around the world.²⁵⁴

²⁴⁷ <<http://www.fashionfantasygame.com/>>.

²⁴⁸ Ibid.

²⁴⁹ Fergus O' Sullivan, 'Is Online Gaming Safe?' (Cloudwards, 12 June 2017) <<https://www.cloudwards.net/is-online-gaming-safe/>> accessed 17 November 2017.

²⁵⁰ Charlie Osborne, 'Millions of Game Accounts Exposed in Data Breach, Responsibility Thrown to the Wind' (ZDNet 20 April 2017) <<http://www.zdnet.com/article/amid-data-breach-responsibility-thrown-to-the-wind/>> accessed 17 November 2017.

²⁵¹ A game where large number of players interact with each other in a virtual world <https://en.wikipedia.org/wiki/Massively_multiplayer_online_role-playing_game> accessed 17 November 2017.

²⁵² <<https://en.gamigo.com/>> accessed 17 November 2017.

²⁵³ Emily Protalinski, '8.24 Million Gamigo Passwords Leaked after Hack' (ZD Net, 23 July 2012) <<http://www.zdnet.com/article/8-24-million-gamigo-passwords-leaked-after-hack/>> accessed 17 November 2017.

²⁵⁴ Ibid.

Data breach is not always caused by a hacker; the information can be leaked accidentally as well. Names and email addresses of thousands of Xbox Live subscribers were accidentally leaked online in March 2013.²⁵⁵ It was unknown if the data fell into the wrong hands, but the subscribers were warned that they could be subjected to potential phishing attacks.²⁵⁶ In December 2014, personal details of more than 13,000 users of the PlayStation, the Xbox and sites including Amazon were leaked online, by the shadowy anarchist group called Anonymous.²⁵⁷ In February 2017 it was revealed that the breach allowed hackers to steal 2.5 million PlayStation and Xbox players' details.²⁵⁸

The next section will investigate whether online users are aware that websites are collecting extensive information from them and that this information may be shared amongst third parties.

2.5. Digital privacy awareness of parents and children

With the explosion of digital technologies, companies are collecting vast quantities of data on consumers' online and even offline activities. Most companies should be open about their data collection, processing and sharing practices contained in the website's privacy policies.

²⁵⁵ Caroline Donnelly, 'Xbox Live Users Hit by Data Breach' (ITPro, 2013) <<http://www.itpro.co.uk/data-leakage/19470/xbox-live-users-hit-data-breach>> accessed 29 March 2016.

²⁵⁶ Ibid.

²⁵⁷ 'Hackers Leak Details of 13k Users of PlayStation, Xbox and Amazon' (*The Telegraph*, 2014) <www.telegraph.co.uk> accessed 29 March 2016.

²⁵⁸ Cara McGoogan, 'Hackers Steal 2.5 Million PlayStation and Xbox Players' Details in Major Breach' (*The Telegraph*, 1 February 2017) <<https://www.telegraph.co.uk/technology/2017/02/01/hackers-steal-25-million-playstation-xbox-players-details-major/>> accessed 4 April 2018.

2.5.1. Parent's digital privacy awareness

According to Global Kids Online,²⁵⁹ children constitute around one-third of the world's internet users.²⁶⁰ As one of the world's largest demographic group using the internet, and with online threats to data privacy, protecting children's digital privacy has become a pressing issue. In the U.S., the Children's Online Privacy Protection Act ('COPPA') requires verifiable parental consent from children under 13 years of age.²⁶¹ According to the Center for Democracy and Training, despite the work of the Federal Trade Commission ('FTC'), online protection of children is still a grave issue.²⁶² The FTC advises parents to stay aware of their children's online activities.²⁶³

Figure 1 represents a study conducted by Lansdowne Market Research²⁶⁴ in 2008. It suggests that 84% of the sample, comprising adults including parents aged 35+, find the privacy of personal information 'very important'.²⁶⁵

²⁵⁹ Global Kids Online works in an international research project that collaborates with UNICEF, the London School of Economics and Political Science (LSE) and the EU Kids Online network to generate cross-national evidence around children's use of the internet. Global Kids Online <<http://globalkidsonline.net/>> accessed 25 April 2018.

²⁶⁰ Ibid.

²⁶¹ Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, section 6502(b)(1)(A)(ii).

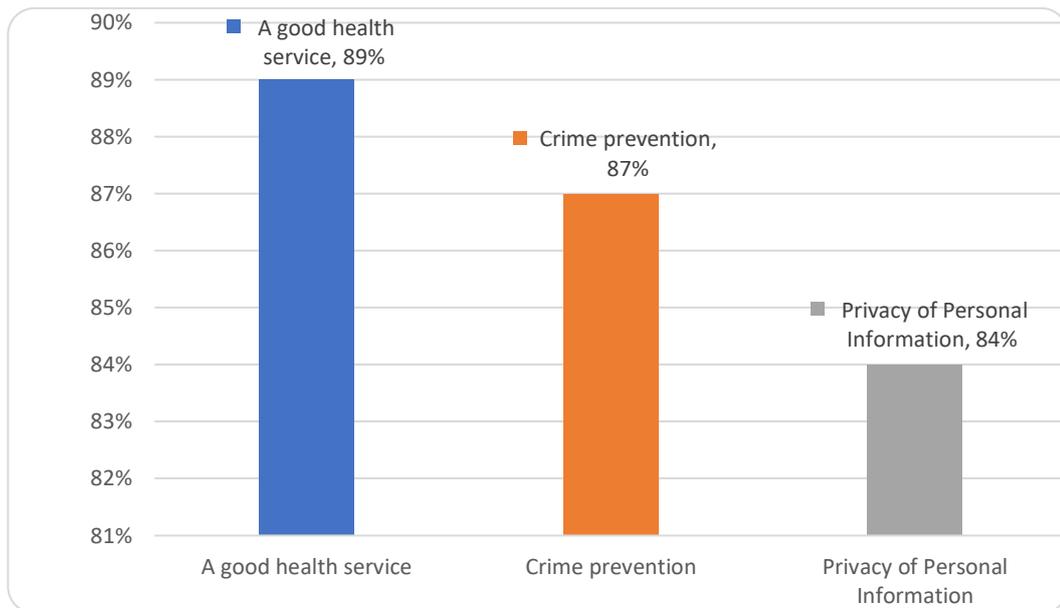
²⁶² H. Raghav Rao and Shambhu Upadhyaya, *Information Assurance, Security and Privacy Services* (Emerald Group Publishing Limited 2009).

²⁶³ 'Complying with COPPA: Frequently Asked Questions' (Federal Trade Commission, 20 March 2015) <<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>> accessed 17 November 2015.

²⁶⁴ Lansdowne Market Research is a market research company that carries out qualitative research to understand the Irish (and European) market <<https://www.greenbook.org/company/Lansdowne-Market-Research>> accessed 18 November 2015.

²⁶⁵ Millward Brown, 'Public Awareness Survey 2008' (Lansdowne Market Research, 2008) <<https://www.dataprotection.ie/documents/trainingandawarenes/PAS08.pdf>> accessed 18 November 2015.

Figure 1 – Privacy of personal information ranks third in order of importance



Source: Landsdowne Market Research

Timothy Morey²⁶⁶ carried out a study revealing that public trust in companies' data sharing practices has fallen,²⁶⁷ with half of the respondents in the study remaining suspicious about how companies used their data.²⁶⁸ Figure 2 shows that although adult users are aware they are under surveillance, they need information about the specific kinds of data that is collected from them and what happens to it.²⁶⁹

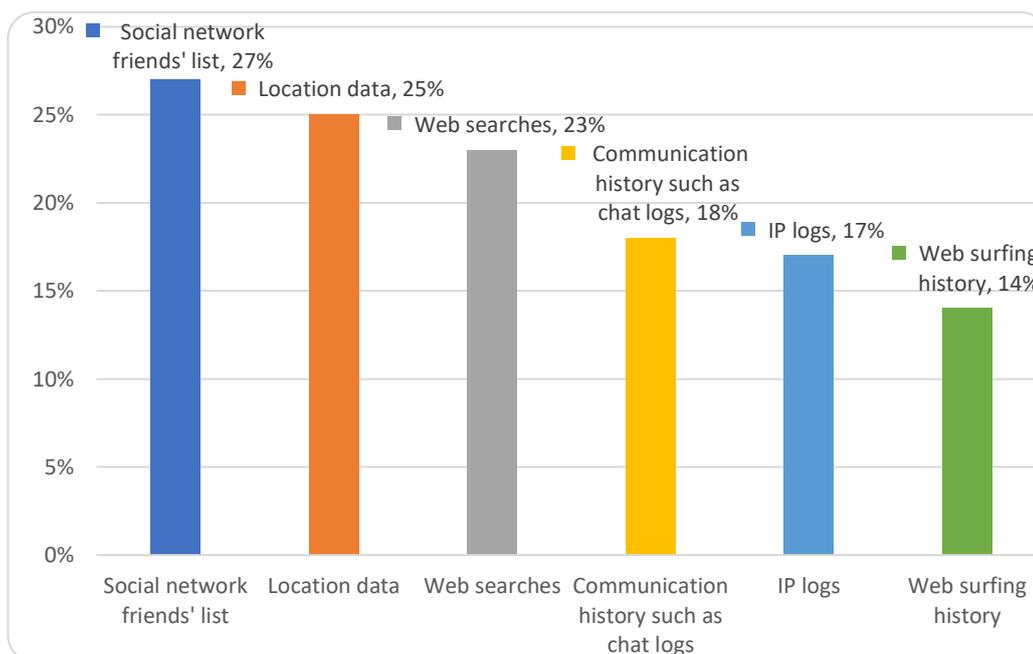
²⁶⁶ Timothy Morey is a vice president of a product strategy and design firm called frog <<https://designmind.frogdesign.com/contributors/timothymorey/>> accessed 29 March 2018.

²⁶⁷ Neil Davey, 'Customer Data Collection: How to Be Trustworthy and Transparent' (MYCustomer, 18 April 2016) <<https://www.mycustomer.com/marketing/data/customer-data-collection-how-to-be-trustworthy-and-transparent>> accessed 27 August 2017.

²⁶⁸ Ibid.

²⁶⁹ Timothy Morey, Theodore 'Theo' Forbath and Allison Schoop, 'Customer Data: Designing for Transparency and Trust' (*Harvard Business Review*, May 2015) <<https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>> accessed 27 August 2017.

Figure 2 Lack of awareness regarding the types of data collection



Source: Landsdowne Market Research

Michael Hsiao and others conducted a study into the parental awareness of parental consent mechanisms and the use of privacy protection tools for parents to protect their children's digital privacy.²⁷⁰ It found that although parents are aware of data collection practices, they have limited legal awareness of the COPPA principles, the legal requirement for websites to obtain verifiable parental consent, and the use of privacy protecting tools such as independent privacy seals (TRUSTe).²⁷¹ Parents admitted to knowing some of the websites their children visited, with vague

²⁷⁰ Michael Hsiao and others, 'Parents and the Internet: Privacy Awareness, Practices and Control' (Amcis, 2007) <<https://pdfs.semanticscholar.org/7a0b/58dfa89fd3b05a221f76006842b3515283c2.pdf>> accessed 17 November 2017.

²⁷¹ TRUSTe is an independent privacy tool, certification of which ensures that the website is incorporating privacy frameworks established by the Federal Trade Commission and the Organisation for Economic Co-operation and Development <<https://www.trustarc.com/privacy-certification-standards/>> accessed 17 November 2015.

identification of whether website operators do anything to protect their children’s data.²⁷²

Figure 3 presents the findings of this study to show the factors that parents will be willing to consider in protecting their children’s digital privacy.

Figure 3 Usage factors parents will take into consideration to protect children’s digital privacy

Parents will use a privacy protection tool if	# of comments	% of comments
1 ... it requires little effort (easy to use)	16	43%
2 ... it is easy to modify its settings	5	14%
3 ... it is needed because the regulations in place protect their child	3	8%
4 ... log files are available (but can be turned on and off)	3	8%
5 ... it gives them more control over the consent they give for sites their children visit	2	5%
6 ... it is efficient to use (cost–benefit)	2	5%
7 ... it provides a list of pre-approved sites (convenience)	2	5%
8 ... it gives them more control over their children’s privacy	1	3%
9 ... they believe that others they know are using it	1	3%
10 ... it is also implemented in schools	1	3%
11... it is downloadable (can’t be lost)	1	3%
Total	37	100%

Source: Landsdowne Market Research

A substantial concern for parents using the internet is the protection of their children’s personal data. Cambridge Analytica’s harvesting of data belonging to 50 million Facebook users²⁷³ reveals that people are willing to give away their personal information without the perceived digital privacy risks. The figures above demonstrate that parents are aware of data gathering practices employed on

²⁷² Michael Hsiao and others, ‘Parents and the Internet: Privacy Awareness, Practices and Control’ (Amcis, 2007) <<https://pdfs.semanticscholar.org/7a0b/58dfa89fd3b05a221f76006842b3515283c2.pdf>> accessed 17 November 2017.

²⁷³ Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted (Channel 4 News, 28 March 2018) <<https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted>> accessed 29 March 2018.

children's websites. They are also aware of the kinds of websites their children visit and have limited understanding of the use of privacy protection tools. It was found that parents are more receptive to privacy tools that are easy to operate (*Figure 3*) They are less aware of the rights and obligations they are entitled to under the operable governing law; the kinds of data extrapolated and the methods whereby website operators ensure children's data remains safe (*Figure 2*) They are interested in protecting their children online but require additional help and support in doing so. One of the ways to achieve this goal is to present a very basic, easy to read privacy policy that clearly explains a parental consent method that is simple to operate.

2.5.2. Children's privacy awareness

Figures 1 and 2 represent the digital privacy awareness of parents, which can be compared with children's digital privacy awareness. EU Kids Online²⁷⁴ carried out a survey of the digital risks experienced by UK children and found significant gaps in children's safety skills, which it recommends the authorities should address.²⁷⁵ Around one-third of 11- to 12-year-olds in the survey cannot block messages from people they don't want to hear from;²⁷⁶ four in 10 nine- to 16-year-olds say the statement 'I know more about the internet than my parents' is 'very true' of them, a quarter say it is 'a bit true' and one-third say it is 'not true' of them.²⁷⁷

²⁷⁴ EU Kids Online is a multinational research network. It seeks to enhance knowledge of European children's online opportunities, risks and safety. EU kids online (LSE 2016)

<<http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>> accessed 7 February 2018.

²⁷⁵ Sonia Livingstone and others, 'Risks and Safety for Children on the Internet: the UK Report' (The London School of Economics and Political Science, December 2010)

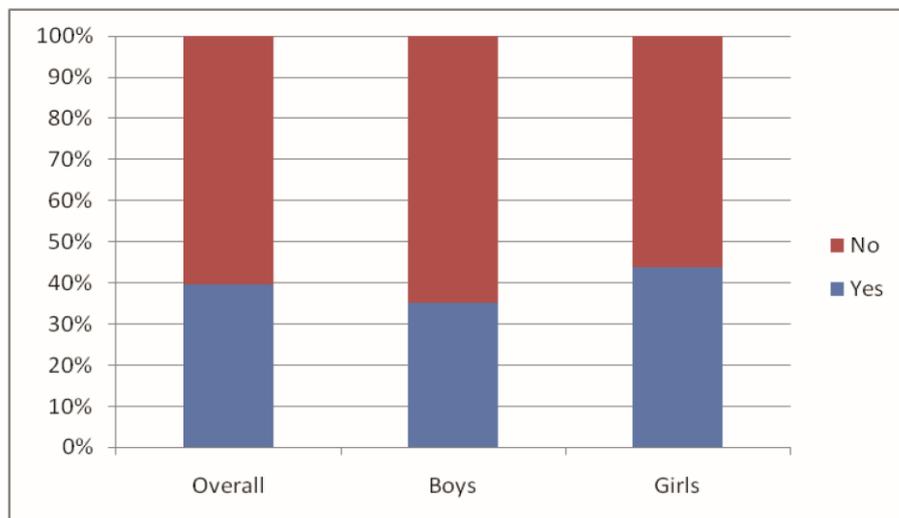
<[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/National%20reports/UKReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf)> accessed 17 November 2017.

²⁷⁶ Ibid.

²⁷⁷ Ibid.

A child privacy report was published by ‘The I in Online’²⁷⁸ on the attitudes of primary school children aged nine to 11 and secondary school children aged 14–19 towards reading website privacy policies. Figure 4 indicates that 60% of the respondents had never read a privacy policy.²⁷⁹ Younger children were less likely to read privacy notices, with 44% of girls more likely to read a privacy policy, a higher percentage than boys, at 35%. It should be noted that the study does not indicate what ‘read’ means. Does it show that the respondents have ticked yes, skimmed through the contents of the privacy policy or read the entire document?

Figure 4²⁸⁰ Privacy policy awareness of children aged 9–11 and 14–19 years old



Source: Landsdowne Market Research

Yes – represents the percentage of children and young people that read privacy policies

²⁷⁸ The I in Online works with the Information Commissioner’s Office and the Irish Data Protection Commissioner’s Office to deliver workshops in schools to children aged 9–11 and 14–19 about the potential pitfalls of sharing too much personal information. ‘Children and Online Privacy Survey’ (The I in Online, 2011) <http://www.chis.org.uk/file_download/49> accessed 17 November 2017.

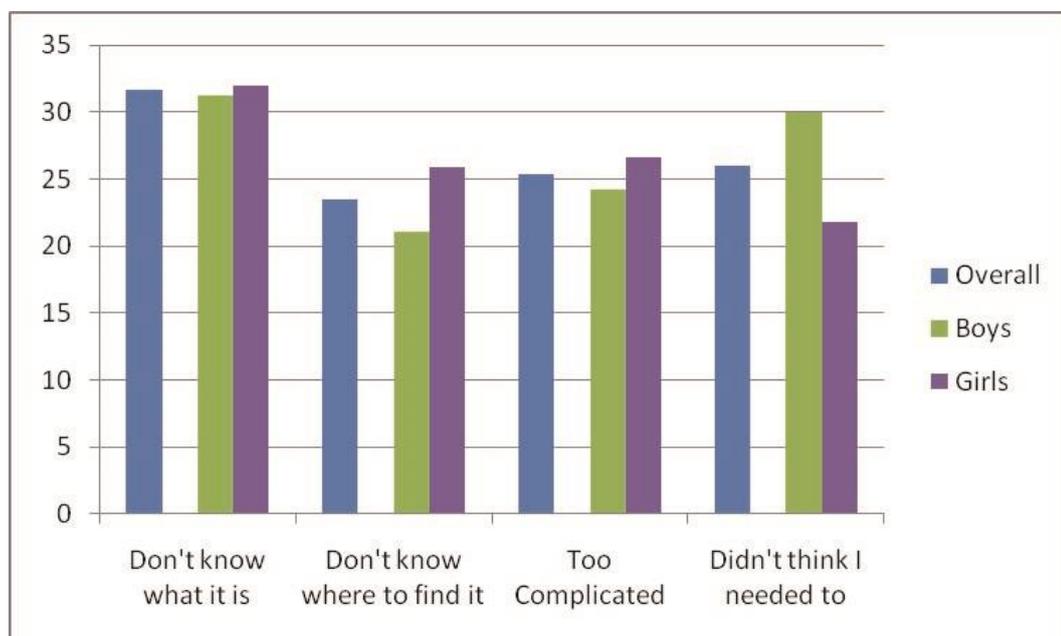
²⁷⁹ ‘Children and Online Privacy Survey’ (The I in Online, 2011) <http://www.chis.org.uk/file_download/49> accessed 17 November 2017.

²⁸⁰ ‘Children and Online Privacy Survey’ (The I in Online, 2011) <http://www.chis.org.uk/file_download/49> accessed 17 November 2017.

No – represents the percentage of children and young people that have never read privacy policies

Figure 5 shows the reasons given by respondents for not reading a privacy policy. A variety of responses were received, with 32% not knowing what a privacy policy was, 23% not knowing where to locate it, and a quarter of the respondents, which interestingly included secondary school children, finding privacy policies unimportant and too complicated to read.²⁸¹

Figure 5²⁸² Reasons for not reading privacy policies



Source: Landsdowne Market Research

From the above, it can be deduced that limited privacy awareness exists amongst children as well as adults when using the internet. Online users are aware of the potential risks to digital privacy, but there is confusion about the kinds of data

²⁸¹ Ibid.

²⁸² Ibid.

collection and the purpose for doing so. Privacy policies are rarely read because they are difficult to find and complicated to read. It is important children and parents be protected through education and using technology to protect themselves online. This can start with ensuring children and their parents can read privacy notices that are accessible and easy to comprehend.

2.5.3. Current policy initiatives on children’s digital privacy rights

Advocates of children’s digital privacy acknowledge the special needs and vulnerabilities of children when using the internet.²⁸³ For instance, in the EU, policymakers and parents are concerned about the implications of online consent. This is due to the presumption that children are more influenced, less critical and therefore more vulnerable than adults, with little experience to guide their judgement.²⁸⁴ The EU GDPR also refers to children as vulnerable natural persons in Recital 75 that maybe exposed to risks of varying severity leading to harm where personal data processing can reveal sensitive information. In the EU, consultations from the UK’s Department for Culture, Media and Sport (DCMS) and the Information Commissioner’s Office (ICO) carried out lengthy discussions on the difficulties experienced by children when online services have a commercial dimension.²⁸⁵

²⁸³ Before the Subcommittee on consumer protection, product safety, and Insurance. Committee on Commerce, Science, and Transportation. United State Senate. Hearing: An examination of children’s privacy: new technologies and the children’s online privacy protection act. (29 April 2010) <<https://www.gpo.gov/fdsys/pkg/CHRG-111shrg66284/pdf/CHRG-111shrg66284.pdf>> accessed 31 January 2018.

²⁸⁴ Ivana Katsarova, ‘Protection of Minors in the Media Environment EU Regulatory Mechanisms’ (Europa 18 March 2013) <[http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130462/LDM_BRI\(2013\)130462_REV1_EN.pdf](http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130462/LDM_BRI(2013)130462_REV1_EN.pdf)> accessed 31 January 2018.

²⁸⁵ Department for Culture, Media and Sport consultation: General Data Protection Regulation – Call for Views (ICO) <<https://ico.org.uk/about-the-ico/consultations/department-for-culture-media-and-sport-consultation-general-data-protection-regulation-call-for-views/>> accessed 31 January 2018.

Particular attention was given to introducing the age of 16 years at which children can provide online consent.

In the U.S., the FTC identified children as ‘sensitive users’ that need special protection.²⁸⁶ The White House’s Consumer Bill of Rights aimed to introduce new policies that require children be provided with special safeguards, but this proposal was later scrapped.²⁸⁷ In practice, few proposals on children’s digital privacy law make it into legislation. An unsuccessful attempt was made to introduce a bill into Congress that would extend the application of COPPA to 13 years and above.²⁸⁸ Calls are being made for the UNCRC to introduce a new set of digital privacy rights that exclusively protect children.²⁸⁹

The previous sections examined the legislative instruments that codify the right to privacy, data breaches in the videogame industry, and privacy awareness of both parents and children. The next section will consider the preliminary legislative instruments to codify data protection and privacy.

²⁸⁶ Federal Trade Commission, ‘Protection Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers’ (FTC, March 2012)

<<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>> accessed 31 January 2018.

²⁸⁷ The White House, ‘Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights’ <<https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b>> accessed 31 January 2018.

²⁸⁸ Belinha S. De Abreu and others, *International Handbook of Media Literacy Education* (Routledge 2017).

²⁸⁹ Sonia Livingstone and Amanda Third, ‘Children and Young People’s Rights in the Digital Age: An Emerging Agenda’ (LSE Research Online) <http://eprints.lse.ac.uk/68759/7/Livingstone_Children%20and%20young%20peoples%20rights_2017_author%20LSERO.pdf> accessed 4 April 2018; Discussion paper series: Children’s Rights and Business in a Digital World (UNICEF) <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 4 April 2018.

2.6. Data protection and privacy codified in legislative instruments

While the right to privacy was taking shape on one side, the early 1980s saw the development of data protection in the EU. This impetus can be traced back to the Organisation for Economic Co-operation and Development Guidelines (OECD Guidelines)²⁹⁰ and the Council of Europe Convention in 1981. The following table lists the chronology of the data protection and privacy law that evolved in the digital environments of the EU and the U.S.

Table 2 – Chronology of global data protection law

Legislation	Year of promulgation	Place of promulgation
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	1980	OECD countries ²⁹¹
Convention for the protection of individuals with regard to automatic processing of personal data	1981	Signatories to the Council of Europe treaty ²⁹²
European Data Protection Directive	1995	EU
Children’s Online Privacy Protection Act	1998	United States
The Charter of Fundamental Rights of the European Union	2000	EU
Treaty on the Functioning of the European Union	2007	EU
Personal Information Protection and Electronic Documents Act	2001	Canada
EU GDPR 2018	2016	EU

²⁹⁰ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>> accessed 20 November 2015.

²⁹¹ Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, France, Finland, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States <<http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm>> accessed 9 December 2017.

²⁹² Fifty countries including Albania, Belgium, Denmark, Germany, France, Italy, Switzerland and the United Kingdom <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures>> accessed 9 December 2017.

2.6.1. Organisation for Economic Co-operation and Development (OECD) Guidelines

The evolution of automatic data processing allowing large volumes of data traversing national frontiers in a matter of seconds made it necessary to consider the privacy protection of personal data. EU member states introduced laws nationally to address this issue, with Germany passing the world's first data protection law in the German Land of Hessen in 1970.²⁹³ This was followed by the German Federal Data Protection Act 1977. The aim of the law was to protect individuals against violations of their personal rights by handling person-related data.²⁹⁴ Sweden created the Data Act in 1973, which was the first national privacy law.²⁹⁵ In 1974, the Council of Europe established Resolutions 73/22 and 74/29 for the protection of personal data in automated databanks.²⁹⁶

There was a possibility for disparities in European member states' national data protection and privacy legislations, which could slow down the free flow of information across borders.²⁹⁷ For this reason, members of the Organisation for Economic Co-operation and Development²⁹⁸ drafted the OECD Guidelines in 1980 to help harmonise laws on data flows across borders.²⁹⁹ The aim of these guidelines is

²⁹³ Albert J. Marcella and Carol Stucki, *Privacy Handbook* (John Wiley & Sons, Inc. 2003).

²⁹⁴ J. Lee Riccardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy* (1983) 6(1) Boston College International and Comparative Law.

²⁹⁵ Sören Öman, *Implementing Data Protection Law* (2004) 47 *Scandinavian Studies in Law*.

²⁹⁶ Sian Rudgard, 'Origins and Historical Context of Data Protection Law'

<https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf> accessed 24 February 2018.

²⁹⁷ OECD, 2013 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

<<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>> accessed 7 April 2016.

²⁹⁸ An organisation of 35 member states that promote policies for the improvement of economic and social well-being of people around the world <<http://www.oecd.org/about/>> accessed 4 April 2018.

²⁹⁹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD)

<<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>> accessed 29 July 2017.

to prevent violations of human rights such as the unlawful storage of personal data, storage of inaccurate data, or the abuse or unauthorised disclosure of data.³⁰⁰

2.6.2. Convention No. 108

One of the earliest attempts to create a legally binding instrument on data protection was Convention No. 108, adopted in 1981 by the Council of Europe.³⁰¹ It created minimum standards for protecting individuals from abuse when their personal data was subjected to collection and processing. Further to this, in 1990 the UN General Assembly also adopted guidelines for the regulation of computerised personal data files.³⁰²

2.6.3. Data Protection Directive 95/46/EC – Now repealed

With the aim to achieve harmony amongst European member states' national data protection and privacy legislations, the EU introduced its comprehensive Directive 95/46/EC to protect individuals' personal data.³⁰³ The Directive regulated the processing of personal data in EU and had to be adopted by member states into their domestic legislation. The United Kingdom implemented its Data Protection Act in 1984, which was then replaced by the Data Protection Act 1998 to implement the provisions of Directive 95/46/EC.

³⁰⁰ Ibid.

³⁰¹ Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, ETS 108, 1981.

³⁰² UN General Assembly Resolution 45/95 of 14 December 1990 Guidelines for the regulation of computerized personal data files 1990 <<http://www.un.org/documents/ga/res/45/a45r095.htm>> accessed 28 November 2015.

³⁰³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2.6.4. The Charter of Fundamental Rights of the European Union

The EU decided to include a list of fundamental rights in a single document, the EUCFR, in December 2000.³⁰⁴ Article 6 of the Treaty on European Union recognised the rights contained in the EUCFR, which has enshrined data protection as a fundamental right under Article 8 ECHR separate from the right to privacy in Article 7 of the EUCFR. This shows that the EUCFR has addressed the protection of personal data as an extension of the right to privacy in the EU.

2.7. Data protection and right to privacy – Two overlapping or separate rights

Beyond the fact that both privacy and data protection are important to preserve societal interests, there is a discord between theorists about whether these two rights can be reconciled. In the opinion of Advocate General Sharpston,³⁰⁵ privacy is a 'classic right' contained in Article 8 ECHR, whereas data protection is a 'more modern right' protected by Convention No. 108,³⁰⁶ like Articles 7 and 8 of the EUCFR. She then recognised the close link between the two rights. In *Google v Spain*,³⁰⁷ the claimant made a complaint that Google should remove his name from appearing in Google search results. The pages contained an announcement for a real estate auction following proceedings for the recovery of debts against the claimant. The court had to consider whether the rights of data subjects extend to requesting that search engines remove personal data.³⁰⁸ It found websites gathering personal

³⁰⁴ Chapters I–VI Charter of Fundamental Rights of the European Union 2000.

³⁰⁵ Markus Schecke and Hartmut Eifert [2010] ECR I -11063 [71].

³⁰⁶ Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data <<https://rm.coe.int/1680078b37>> accessed 26 November 2015.

³⁰⁷ *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González C-*[2014] Case 131/12.

³⁰⁸ *Ibid* [19], [62], [63].

information for profit should remove links to private information when it is no longer relevant.³⁰⁹

Privacy and data protection have been regarded as two distinct rights by legal theorists Christina Akrivopoulou and Athanasios-Efstratios Psykgassince.³¹⁰ They are endorsed as two different fundamental rights under Article 7 (right to privacy) and Article 8 (protection of personal data) of the EUCFR and Article 8 (right to privacy) of the ECHR. Interference with privacy rights is allowed if certain conditions are satisfied under Article 52(2) of the EUCFR and Article 8(2) of the ECHR, respectively.

The right to privacy deals with privacy of individuals, while data protection laws relate to the processing of personal data if it satisfies certain safeguards. Therefore, from a formal point of view they are very separate. It can be questioned whether the right of access and correction, a supervisory authority and the requirement of legitimate and fair processing strictly fall within the ambit of the right to privacy. For instance, the European Court decided in *Goodwin v United Kingdom* that, although there was breach of Article 8 ECHR, it did not expressly entitle a transsexual to rectify gender.³¹¹ The right to privacy will potentially protect the personal boundaries of an individual irrespective of whether data processing is involved or not.

The legal right of privacy cannot be contained in an exhaustive list because people should be able to live with liberty and autonomy without any arbitrary interference in their private sphere.³¹² But, on the other hand, data protection does not mean that

³⁰⁹ Ibid [99].

³¹⁰ Christina Akrivopoulou and [Athanasios](#) Psygkas, *Personal Data Privacy and Protection in a Surveillance era: Technologies and Practices* (IGI Global 2011).

³¹¹ *Goodwin v United Kingdom*, no. 28957/95, 11 July 2002 [92].

³¹² Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193 <<http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>> accessed 24 March 2016.

data processing activities will be limited. Instead, there should be a free flow of information³¹³ between member states,³¹⁴ which makes the two rights different from a substantive point of view as well.³¹⁵

The concepts can have both a broad and narrow interpretation. Data protection can be interpreted narrowly, because it only deals with the protection of personal data. It can have broad implications as it not only affects an individual's digital privacy but also influences other fundamental rights such as freedom of expression, religion and reputation.³¹⁶

The right to privacy is wide as it encompasses a non-exhaustive list. And it can be limited by conditions justifying interference by the state under Article 8(2) ECHR. Data protection and privacy are capable of dual interpretations but there is guidance in the European Court of Justice's ('ECJ') decisions in *Promusicae*³¹⁷ and *LSG Order*³¹⁸ that, where the rights are different, interpretation must be done in a way that allows

³¹³ Daniel Guagnin and others, *Managing Privacy through Accountability* (Palgrave Macmillan 2012).

³¹⁴ Directive 95/46/EC Article 1(2).

³¹⁵ Daniel Guagnin and others, *Managing Privacy through Accountability* (Palgrave Macmillan 2012).

³¹⁶ *Ibid* 269.

³¹⁷ *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] Case C-275/06 [70].

Promusicae is an organization of producers and publishers of musical recordings. It was able to identify the IP (internet protocol) addresses of people that were sharing files to which Promusicae held exclusive rights. Promusicae wanted to identify the users behind the IP addresses to initiate civil proceedings. The court decided that the European Community Directives 95/46/EC and 2002/58 allow member states to adopt legislative measures that restrict confidentiality 'when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, public security...'

³¹⁸ *Tele 2* is an internet service provider that assigned dynamic IP addresses to users. LSG applied to the Austrian court for an order requiring Tele 2 to send names and addresses of persons to whom it had provided internet access service and whose IP addresses and date and time of connection were known. Tele 2 stated that it is not an intermediary and is not authorised to save access data. The court was faced with the question of whether the copyright rules will apply to an access provider who merely allocates a dynamic IP address and not any other services such as email, FTP or file-sharing services. The provider does not even exercise any control over the services which the user makes use of. *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] Case C-557/07 [28].

‘a fair balance between the various fundamental rights protected by the legal order’.³¹⁹

Furthermore, Article 8(3) of Directive 2004/48/EC,³²⁰ read in conjunction with Article 15(1) of Directive 2002/58/EC,³²¹ does not preclude member states from imposing an obligation to disclose to private third parties, personal data relating to internet traffic that will enable them to bring civil proceedings for copyright infringements.³²²

2.8. Conclusions

The right to privacy is a broad concept that has been interpreted in diverse cultures to mean different things. The right to privacy has branched into various other rights such as data protection, which is a comparatively novel right and remains in a phase of development. Data privacy law needs to keep pace with technological advancements but usually lags. It is still in a process of being understood as jurists have remained at loggerheads in determining whether the two rights are separate or overlap.

It has been identified that parents are both interested in protecting their children online and are aware of data gathering practices employed on websites. But they have limited technical awareness regarding complex privacy protection tools, the kinds of data collected, data privacy law and the methods whereby website operators protect children’s personal data. Therefore, a requirement of parental consent is

³¹⁹ Steeve Peers and others, *The EU Charter of Fundamental Rights* (Hart Publishing Ltd 2014).

³²⁰ Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004).

³²¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

³²² *Ibid* 29.

insufficient if information is not provided to parents in a readily comprehensible manner. It is proposed that to improve parents and children's digital privacy awareness, they should be presented with easy to read and simple privacy policies. The parental consent method should be explained in plain language and easy to operate. The website operator should facilitate parents with simple information that is easy to grasp so that they can make informed decisions.

The next chapter will critically analyse the principles of the main data protection and privacy laws in EU that protect the processing of European citizens' personal data, i.e. the now repealed Directive 95/46/EC and Directive 2002/58/EC (the 'e-Privacy Directive')³²³ and EU GDPR 2018³²⁴ (which will replace Directive 95/46/EC) to determine if the proposed changes overcome the shortcomings identified in Directive 95/46/EC.

³²³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

³²⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Text with EEA relevance).

CHAPTER THREE

EUROPEAN DIGITAL PRIVACY LEGISLATION

3.1. Introduction

Chapter 2 discussed the preliminary legislation that codified the right to privacy and data protection, the privacy awareness of users and the relationship between the two rights. This chapter critically analyses the principles of the current and prospective data protection and privacy legislation in EU.

Section 3.1.2 presents the preliminary observations that the age at which children consent differ between jurisdictions. Section 3.2 examines the main principles of the now repealed Data Protection Directive³²⁵ ('Directive 95/46/EC') and the EU GDPR 2018.³²⁶ Section 3.3 examines the e-Privacy Directive³²⁷ and its provisions on laws regulating cookies placed on users' devices. Section 3.4 provides a concluding analysis of this chapter and preliminary findings significant for the first part of the multiple case study in *Chapter 5*.

Chapters 3 and 4 of this thesis carries out the doctrinal legal research as part of the research methodology selected for this thesis. The two chapters evaluate the legal

³²⁵ European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (Council of Europe 4 November 1950) <<http://www.refworld.org/docid/3ae6b3b04.html>> accessed 24 March 2016.

³²⁶ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2012.

³²⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

principles that regulate a website's data handling practices in the legislation in the EU, the U.S. and Canada. This analysis will uncover essential characteristics of data privacy frameworks, which can be applied to the multiple case study of privacy policies to determine their compatibility with governing laws.

3.1.1. Europe's response to the emerging threat of digital privacy

Chapter 2 considered the international legal instruments as well as the opinions of legal jurists' understandings of the rights to data protection and privacy.

As well as the concerted legislative efforts to codify data protection, the Council of Europe Convention³²⁸ was an international effort to create a binding instrument that regulates the transborder flow of personal data.³²⁹ Such attempts led to the adoption of the Data Protection Directive 95/46/EC,³³⁰ which was the most important piece of European data privacy legislation before the EU GDPR 2018. Directive 95/46/EC encompassed key elements of the right to privacy under Article 8 of the European Convention on Human Rights (ECHR)³³¹ and the Organisation for Economic Co-operation and Development (OECD Guidelines).³³² The inclusion of data protection

³²⁸ 81/679/EEC: Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Europa) <<https://publications.europa.eu/en/publication-detail/-/publication/d664d1d0-832e-4341-a1bf-7af18d09d9b5/language-en>> accessed 7 April 2016.

³²⁹ Details of Treaty No. 108 (Council of Europe) <<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>> accessed 7 April 2016.

³³⁰ European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³³¹ European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (Council of Europe 4 November 1950). <<http://www.refworld.org/docid/3ae6b3b04.html>> accessed 24 March 2016.

³³² OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD) <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>> accessed 24 March 2016.

as an autonomous fundamental right shows the importance that EU law attaches to the technological progress occurring online.³³³

The next section will present a preliminary observation concerning the inconsistent ages at which children can provide consent in different jurisdictions.

3.1.2. The range of age for consent differ in international jurisdictions

This thesis considers the data privacy rights of children. For this purpose, a child is anyone under the age of 18 years. This recommendation is compatible with international obligations created by the United Nations Charter of Fundamental Rights.³³⁴ It was difficult to determine the exact legal definition of a child and the age at which children can provide legal consent. This is because there is discrepancy amongst jurisdictions on the age of consent. This discord can create confusion on the possible privacy protection accorded to children when playing videogames registered in other jurisdictions.

The UN Convention on the Rights of Child (UNCRC) defines a 'child' as anyone under the age of 18 years.³³⁵ Directive 95/46/EC remained silent on the age at which children can provide consent for digital processing of their personal data.³³⁶ Part of

³³³ '2010 Data Protection in European Union: the role of National Data Protection Authorities' (Europa) <<http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities>> accessed 24 March 2016.

³³⁴ UNCRC Article 1 defines a child as anyone under the age of 18 years.

³³⁵ Article 1, UN Convention on the Rights of the Child.

³³⁶ Article 29 EU Data Protection Working Party, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (Europa, 11 February 2009) <http://webcache.googleusercontent.com/search?q=cache:T2kmKrBlUbgJ:ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=2&hl=en&ct=clnk&gl=uk> accessed 14 April 2018.

the reason behind this differential application is because the Directive allowed member states some autonomy in determining their own rules.³³⁷

Both Korff and Dowty carried out a study in EU relating to the consenting age and found broad discrepancies.³³⁸ For instance, in the UK children over 16 can give consent, but public authorities have advised in guidance that a child of around 12 is usually competent for consenting to information sharing.³³⁹ Korff and Dowty stringently requested that any references to the age of 12 years be removed immediately and the age of consent be extended to 16 years.³⁴⁰

In some member states, such as Germany, the data controller will have to judge effective consent by looking at the degree of maturity exhibited by the child; similarly, children should be able to understand the content, scope and potential consequences of their consent.³⁴¹ In *Lüneburg*,³⁴² the judges held that consent will not be valid if the child was under 14 years of age. Children should be able to understand the consequences of processing, and in many instances, parents will be consulted.³⁴³

In France, although the age of majority is 18 years, children can enter into marriage at the age of 15 with at least one parent's consent and can obtain a bank (ATM) card

³³⁷ Ibid 19.

³³⁸ Terri Dowty and Douwe Korff, 'Protecting the Virtual Child: The Law and Children's Consent to Sharing Personal Data (ARCH 2009)' <http://www.northumbria.ac.uk/static/5007/hces/virtual_child.pdf> accessed 10 January 2016.

³³⁹ Ibid.

³⁴⁰ Ibid 12.

³⁴¹ Norbert Nolte and Christoph Werkmeister, 'Data Protection in Germany: An Overview' (Practical Law) <<http://uk.practicallaw.com/3-502-4080>> accessed 15 May 2016.

³⁴² *Germany, Case No. 11 LC 114/13*.

³⁴³ Carlo Piltz, 'The European Data Protection Law and Minors – No Legal Certainty' (German IT Law, 2014) <<http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty/>> accessed 12 January.

at 12 years. Some states such as Spain have tried to benefit from the relative autonomy that was given by the earlier Directive 95/46/EC in formulating a parental consent mechanism.³⁴⁴ Many websites are required to restrict access to children under 14 years, by putting in place age-gating mechanisms.³⁴⁵

The EU GDPR 2018 is applicable uniformly in member states, but it does not provide complete harmonisation on the aspect of age for consent. Article 8³⁴⁶ requires verifiable parental consent from children under 16 years of age. But member states are allowed discretion to lower the age to 13 years. This will perpetuate the uncertainty around the age at which children can provide online consent. EU GDPR 2018 does not provide methods for obtaining parental consent. Instead, it requires the controller to take reasonable efforts in verifying that the parent has given consent for processing the child's data.³⁴⁷

There is also discrepancy in the age for consent in the US data privacy law. The Children's Online Privacy Protection Act (COPPA) operates on a nationwide level³⁴⁸ and applies to videogame websites directed to children under 13 years of age.³⁴⁹ Individual states have enacted additional data privacy laws to complement the work of COPPA. For instance, the Delaware Online Privacy Protection Act defines a child as anyone under the age of 18 years.³⁵⁰

³⁴⁴ Kingdom of Spain, Royal Decree 1720/2007 of 21 December approving the Regulations implementing Law 15/1999 on the Protection of Personal Data 2007, Article 13(1).

³⁴⁵ 'Children's Data Protection and Parental Consent' (Advertising Education Forum, 2013) <<http://www.socialwebsocialwork.eu/content/research/index.cfm/action.showfull/secid.25/ndcdc.11/ndc.1030/key.1030>> accessed 15 January 2016.

³⁴⁶ EU GDPR 2018.

³⁴⁷ EU GDPR 2018 Article 8(2).

³⁴⁸ Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505.

³⁴⁹ 16 CFR §312.2.

³⁵⁰ Delaware Online Privacy Protection Act s 1202C (6).

Issues will be created if a 16-year-old child in Delaware plays an online videogame registered in Spain, where the age of consent is 14 years. For the purposes of Spain, the child from Delaware will be treated as an adult and the special requirements to protect children online will not be extended to her.

It is important that data privacy regimes decide on a universal age of consent rather than allow states to exercise discretion. It is proposed that jurisdictions ought to define a child as anyone under the age of 18 years and should treat them as a special class of data subject requiring additional online protection. It would be unreasonable to subject 18-year-old children to parental consent mechanisms. Therefore, it is recommended that children under 16 years should provide verifiable parental consent. This is compatible with the definition of a child given by the UNCRC and the EU GDPR 2018 requirement that parental consent will be needed when processing personal data of children under 16 years.³⁵¹

3.2. Data Protection Directive 95/46/EC – now repealed

The key European data protection directives governing the use of personal data collected online are the now repealed Directive 95/46/EC, the e-Privacy Directive,³⁵² which regulate the processing of data and smart tracking technologies (cookies), respectively and the EU GDPR 2018 which is in force since 25th May 2018.

Directive 95/46/EC was not implemented uniformly across member states, owing to varying cultures, languages and legal systems. The aim to achieve harmony, the need

³⁵¹ EU GDPR 2018 Article 8(1).

³⁵² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

to remain abreast with technological developments and the risks posed by the internet in potentially endangering an individual's online privacy led the European Commission to draft the EU GDPR 2018.³⁵³

In January 2012 the European Commission proposed a reform of Directive 95/46/EC to strengthen digital privacy rights and boost the EU's digital economy.³⁵⁴ A study into the digital economy and the level of trust demonstrated unsatisfactory results among users. In fact, the study commissioned by the European Commission questioning 1,000 SMEs (small and medium-sized enterprises) about the '10 most burdensome EU laws' resulted in data protection laws ranking in seventh place.³⁵⁵

The European Commission believes that the EU GDPR 2018 modernises the law, provides greater protection to data subjects and allows for harmonisation. This is strongly contested by the British minister of justice, who claims that the costs to British companies alone will be between £250 million and £300 million per year.³⁵⁶

The EU GDPR 2018 took effect on 25th May 2018 across European member states.³⁵⁷ It has direct application³⁵⁸ of data protection rules in the member states by facilitating harmonisation, legal certainty and transparency of the law.³⁵⁹ The EU GDPR 2018 has

³⁵³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Text with EEA relevance).

³⁵⁴ 'Reform of the EU Data Protection Legal Framework in the EU' (europa) <https://ec.europa.eu/info/law/law-topic/data-protection/reform_en> accessed 7 December 2015.

³⁵⁵ 'Commission Wants to Simplify Life for SMEs by Easing the Top 10 Most Burdensome EU Laws' (Europa 2013) <http://europa.eu/rapid/press-release_IP-13-188_en.htm> accessed 8 December 2015.

³⁵⁶ 'Impact Assessment' (Ministry of Justice, 2012) <<https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf>> accessed 9 December 2015.

³⁵⁷ 'Reform of EU Data Protection Rules' (Europa) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 10 December 2017.

³⁵⁸ 'Reform of EU Data Protection Rules' (Europa) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 7 April 2016.

³⁵⁹ Online Privacy Law: European Union (Library of Congress, 2015) <<http://www.loc.gov/law/help/online-privacy-law/eu.php>> accessed 5 December 2015.

not stirred the pot of definitions, which largely remain the same as in the earlier Directive 95/46/EC.³⁶⁰

It has introduced additional elements in treating children as a special class of data subjects,³⁶¹ strengthening the concept of consent,³⁶² the transparency principle,³⁶³ the liability of the controller,³⁶⁴ clarification of the data minimisation principle³⁶⁵ and the one-stop shop rule,³⁶⁶ and the right to be forgotten features prominently.³⁶⁷

Main principles of the now repealed Directive 95/46/EC for processing personal data

The main principles of Directive 95/46/EC are dealt with separately. The changes proposed by the EU GDPR 2018 will be presented to determine the effectiveness of the new law.

³⁶⁰ Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (EDPS, 2014) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf> accessed 7 April 2016.

³⁶¹ A child aged 16 years can provide online consent. Children under 16 years will have to furnish verifiable parental consent. EU GDPR 2018 Article 8.

³⁶² Consent has to be a written declaration which has to be presented in a clearly distinguishable, intelligible and easily accessible manner, using clear and plain language. EU GDPR 2018 Article 7.

³⁶³ The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, that it is in clear and plain language and, additionally, where appropriate, visualisation be used. EU GDPR 2018 Recital 58; EU GDPR 2018 Article 5(1)(a).

³⁶⁴ It is the controller's responsibility to ensure to implement appropriate technical and organisational measures and demonstrate that processing is performed in accordance with this Regulation. EU GDPR 2018 Article 24.

³⁶⁵ Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. EU GDPR 2018 Article 5(1)(c).

³⁶⁶ The one-stop shop rule applies where a single controller or processor operates across more than one member state or, if operating in a single member state, engages in processing that is likely to substantially affect individuals in more than one member states. Article 29 EU Data Protection Working Party, 'Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority' (Europa, 13 December 2016) <[file:///C:/Users/User%201/Downloads/wp244_rev01_enpdf%20\(1\).pdf](file:///C:/Users/User%201/Downloads/wp244_rev01_enpdf%20(1).pdf)> accessed 4 April 2018.

³⁶⁷ The data subject should be able to obtain from the controller the erasure of personal data concerning him or her. EU GDPR 2018 Article 17. Francoise Gilbert, 'EU Data Protection Overhaul: New Draft Regulation' (Global Privacy Book) <<http://www.globalprivacybook.com/blog-european-union/223-eu-data-protection-overhaul-new-draft-regulation>> accessed 10 December 2015.

From the very outset, Article 1 of Directive 95/46/EC required member states to protect the right to privacy of European citizens with respect to the processing of personal data. This principle presented various terms that need to be explained. The most obvious are 'personal data' and 'processing'.

3.2.1. Definition of 'processing' and 'personal data'

According to the earlier Directive 95/46/EC, personal data referred to 'any information relating to an identified or identifiable natural person' either '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'.³⁶⁸ Processing of personal data applied to the 'collection, recording, organization, storage ... erasure or destruction' of personal data.³⁶⁹ The definition of personal data introduced additional terms: 'relate to' and 'identified or identifiable', which will be considered in turn.

3.2.1.1. Meaning of the phrase 'relate to'

Any information will 'relate to' the individual to become personal data.³⁷⁰ The UK's Information Commissioner³⁷¹ found that data had to be 'absolutely about' an

³⁶⁸ Directive 95/46/EC Article 2(a).

³⁶⁹ Directive 95/46/EC Article 2(b); Special categories of data ('sensitive data') such as information revealing ethnic origin, religious beliefs and health require additional protections including explicit consent. Directive 95/46/EC Article 8.

³⁷⁰ Directive 95/46/EC Article 2(a); From an objective point of view, any information will 'relate to' a person when it is about that person 2012. 'Determining What Is Personal Data' (ICO) <<https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>> accessed 8 April 2016.

³⁷¹ 'The UK's Independent Authority Set Up to Uphold Information Rights in the Public Interest, Promoting Openness by Public Bodies and Data Privacy for Individual' (ICO) <<https://ico.org.uk/>> accessed 30 June 2017.

individual and mere references will not 'relate to' and therefore not amount to personal data.³⁷²

In *Durant v Financial Services Authority*,³⁷³ the court preferred a narrow approach, stating that the 'mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data'³⁷⁴ unless it is accompanied by additional information such as address, telephone number, hobbies etc.³⁷⁵

3.2.1.2. Definition of 'identified' or 'identifiable'

Personal data should either be 'identified' or 'identifiable' to an individual³⁷⁶ through a name or combination of other factors such as the individual's address, picture or parents' names.³⁷⁷

The next section considers whether the EU GDPR 2018 ensures harmony amongst member states in applying the definition of personal data.

³⁷² 'Determining What Is Personal Data' (ICO, 2012) <<https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>> accessed 5 December 2015.

³⁷³ *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

³⁷⁴ *Ibid* 28.

³⁷⁵ 'The "Durant" Case and Its Impact on the Interpretation of the Data Protection Act 1998' (Information Commissioner) <<http://www.nhsgrampian.org/grampianfoi/files/DurantCase.pdf>> accessed 6 December 2015.

³⁷⁶ Directive 95/46/EC Article 2(a).

³⁷⁷ Article 29 EU Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (Europa, 2007) <<https://webcache.googleusercontent.com/search?q=cache:hk6F0jzjTOUJ:https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2016/05/19/ek-bijlage-2-definitie-anonieme-gegevens-algemene-verordening-gegevensbescherming/ek-bijlage-2-definitie-anonieme-gegevens-algemene-verordening-gegevensbescherming.pdf+&cd=2&hl=en&ct=clnk&gl=uk>> accessed 6 December 2015.

3.2.1.3. EU GDPR 2018 on the definition of ‘personal data’

The EU GDPR 2018 includes ‘online identifiers’³⁷⁸ in the definition of personal data.³⁷⁹

Recital 23 of the EU GDPR 2018³⁸⁰ also adds ‘that a person must be considered identifiable when either the data controller or another natural or legal person can identify the person’.

The inclusion of the terms ‘natural or legal person’ broadens the horizon for casting a bigger safety net and securing anyone as ‘identifiable’.

3.2.2. Definition of ‘controller’ and ‘processor’

Article 2(d) of Directive 95/46/EC defined the data controller as any natural, legal person or authority that determines who should comply with data protection rules and how data subjects would exercise their rights in practice. The processor on the other hand has the responsibility of identifying those involved in the processing of personal data.³⁸¹ For the purposes of this thesis, the data controller will be referred to as the ‘website operator’.

The following sections will list the principles before the legitimate processing of personal data can occur.

³⁷⁸ Any identifier that you would use for the purpose of online communication. This would include a screen name if you posted in an online forum or a login you used for an application or website through which you communicate and can include email address, instant chat. <<https://floridaactioncommittee.org/question/internet-identifier-exactly-required-registered/>> accessed 10 December 2017.

³⁷⁹ Frederik Zuiderveen Borgesius, ‘Behavioral Targeting, a European Legal Perspective’ (2013) 11(1) IEEE Security & Privacy 82, 82–85.

³⁸⁰ European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012.

³⁸¹ Article 29 EU Data Protection Working Party, ‘2010 Opinion 1/2010 on the Concepts of “Controller” and “Processor”’ (Europa) <<http://webcache.googleusercontent.com/search?q=cache:132kmgLH1xYJ:www.pdpjournals.com/docs/88016.pdf+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 11 December 2015.

3.2.3. Principles of data processing – data quality

Article 6(2) of Directive 95/46/EC provided that ‘it shall be for the controller to ensure that paragraph 1 is complied with’. Paragraph 1 refers to all the main principles relating to data quality. These principles will be dealt with separately and the ensuing amendments contained in the EU GDPR 2018 will be discussed as well.

The first requirement for processing of personal data is that it must be processed fairly and lawfully under Article 6(1)(a).³⁸²

3.2.3.1. Meaning of the phrase ‘fairly and lawfully’

Author Lee A. Bygrave states that the notion of fairness requires the data controller to take account of interests and reasonable expectations of data subjects,³⁸³ but very few data protection instruments address this issue.³⁸⁴ What are the reasonable expectations of a child data subject with limited privacy awareness? What about the fact that Google has admitted to mining millions of student emails through its apps for education used in schools worldwide without the children, their parents and even the school authorities’ consent, despite promises of privacy?³⁸⁵

There is a need to clarify the exact limits of the term ‘fairly’, which can be susceptible to broad notions, so that data subjects know what to expect and businesses can understand and acknowledge their boundaries.

³⁸² Directive 95/46/EC.

³⁸³ Lee. A. Bygrave *Data Protection Law* (Kluwer Law International 2002).

³⁸⁴ *Ibid.*

³⁸⁵ Samuel Gibbs, ‘Google Accused of Spying on Students in FTC Privacy Complaint’ *The Guardian* (2 December 2015) <<http://www.theguardian.com/technology/2015/dec/02/google-eff-ftc-privacy-chromebook-gmail-spying-students>> accessed 27 December 2015.

3.2.3.2. Meaning of the phrase ‘collected for a specified purpose’

Also known as the principle of ‘purpose specification’, data should be gathered for a specified, legitimate and compatible purpose.³⁸⁶ Users should be informed as to why their personal data is collected and the specified purpose behind the collection, processing and storage.³⁸⁷ According to Article 29 EU Data Protection Working Party (Art29 WP),³⁸⁸ statements such as ‘improving user experience’ or ‘marketing purposes’ will not suffice for ‘specified, explicit and legitimate purposes’ because it is too vague.³⁸⁹ After this, the next stage is where the user will consent. An individual’s informed consent to processing personal data will depend upon the information behind the purpose of using personal data. This will also assist users in tracing the entity responsible for maintaining their information. However, data sharing practices in some instances disregard this principle.

The Thomas and Walport Data Sharing Review³⁹⁰ exposed the absence of clarity in the legal justification of data sharing and the lack of accountability and transparency found in the process.³⁹¹

³⁸⁶ Directive 95/46/EC Article 6(1)(b); EU GDPR 2018 Article 5(1)(b).

³⁸⁷ Directive 95/46/EC Article 6(1)(b); Recital 28.

³⁸⁸ Article 29 EU Data Protection Working Party is an independent advisory body that seeks to harmonise data protection rules across EU and publishes opinions and recommendations on various data protection and privacy topics. It comprises representatives from the data protection authority of each EU member state. Office of the Data Protection Commissioner, ‘Article 29 Working Party’ (Data Protection Commissioner) <<https://www.dataprotection.ie/docs/Article-29-Working-Party/u/181.htm>> accessed 5 April 2018.

³⁸⁹ Article 29 EU Data Protection Working Party, ‘Opinion on 3/2013 on Purpose Limitation’ (Europa, 2 April 2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 21 September 2017.

³⁹⁰ Mark Walport and Richard Thomas, ‘Data Sharing Review Report’ (Ministry of Justice 2008).

³⁹¹ Ibid 46–48.

The EU GDPR 2018 reiterates this principle but also adds that data subjects can essentially hold the data controller responsible for any kind of data and security breach.³⁹²

3.2.3.3. Meaning of the phrase ‘adequate, relevant and not excessive’

Contained in Article 6(1)(c) of Directive 95/46/EC, the principle of minimality limited data collection to achieve the purpose behind the collection. However, privacy policies have allowed websites directed at children to collect extensive information that will fall against individual interests.³⁹³

The provision also effectively required personal data to be erased or anonymised once it is no longer needed.³⁹⁴ In some website privacy policies, the information will be retained for ‘as long as is reasonably necessary’, which is not compatible with the above principle.

While not a novel concept, ‘data minimisation’ has been emphasised in the EU GDPR 2018, signalling that data can only be collected for a task and consent will be required before data is repurposed.³⁹⁵ This will place onerous burdens on controllers and it will be interesting to see how it is implemented.

One of the requirements for data processing is that it should be based on legitimate interests.

³⁹² ‘What Is the EU General Data Protection Regulation?’ (Strategicrisk, 2015) <<http://www.strategic-risk-global.com/what-is-the-eu-general-data-protection-regulation/1416820.article>> accessed 17 December 2015; EU GDPR 2018 Article 24. It will ultimately be the controller’s responsibility to ensure compliance with the provisions of EU GDPR 2018.

³⁹³ Tobias Mahler, Lothar Fitsch and Audun Josang, ‘Privacy Policy Referencing’ (2010) <<http://folk.uio.no/josang/papers/JFM2010-TrustBus.pdf>> accessed 17 December 2015.

³⁹⁴ Directive 95/46/EC Article 6(1)(e).

³⁹⁵ EU GDPR 2018 Article 5(1)(c).

3.2.3.4. Definition of 'legitimate interests'

One of the most flexible lawful basis for processing, the controller will have to identify a legitimate interest, show that processing is necessary to achieve it and thirdly carry out a balancing test between the legitimate interests of the data controller against the fundamental rights and freedoms of the data subject.³⁹⁶ The Art29 WP believes that the notion of legitimate interests can comprise a multitude of interests such as freedom of expression or information, direct or other forms of marketing and advertisements.³⁹⁷

The earlier Directive 95/46/EC provided little guidance on determining what interests are 'legitimate' and when can it be overridden by the interests of the data subject.³⁹⁸

In reality, the legitimate interest provision is regularly utilised by data controllers to defend data processing. One of the most commonly occurring forms of abuse is where privacy policies and terms of service (TOS) contracts are framed broadly. The website operator defends the wide wording based on their legitimate interests, which are difficult to follow by the user.

3.2.3.5. EU GDPR 2018 on 'legitimate interests'

The EU GDPR 2018 has narrowed the principle down by allowing processing only if it is in the interests of the data controller and unless such interests were overridden by

³⁹⁶ Directive 95/46/EC Article 7(f); Article29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (Europa, 9 April 2014) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 10 May 2016; 'Legitimate Interests' (ICO) <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>> accessed 5 April 2018.

³⁹⁷ Ibid.

³⁹⁸ 'A Loophole in Data Processing' (Bits of freedom, 11 December 2012) <https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf> accessed 10 May 2016.

the fundamental rights of the data subject requiring data protection, and when the data subject is a child.³⁹⁹

Processing of data based on legitimate interests will be allowed ‘in the public interest or scientific, statistical or historical purposes’.⁴⁰⁰ It is unclear what these statistical and scientific purposes are because a website that processes personal data of children for profit could easily claim that it is processing data for scientific purposes.

3.2.4. Information to be given to children when processing personal data

Privacy notices such as privacy policies, terms and conditions and/or EULAs are meant for avoiding any liability.⁴⁰¹ But the sheer length and complex legalistic terminology means they are hardly ever read.⁴⁰² People should be facilitated with simple and easy models to help them decide. But, as consent becomes more and more complicated, it is difficult to see how the data subject will consent while retaining all the different considerations in mind.

EU Directive 95/46/EC required website operators to provide the data subject with information relating to the identity of the controller, the purpose of processing, the categories of data collected and the right of rectification.⁴⁰³ This information was ideally suited for a privacy policy, but the Directive did not specify this. It lacked

³⁹⁹ EU GDPR 2018 Article 6(f).

⁴⁰⁰ EU GDPR 2018 Article 6(2).

⁴⁰¹ Jordan Nahmias, ‘The EULA: What It Does, How It Works (and, What Does EULA Even Mean?)’ (Nahmiaslaw, 23 November 2011) <<http://www.nahmiaslaw.com/the-eula-what-it-does-how-it-works-and-what-does-eula-even-mean/>> accessed 16 May 2016.

⁴⁰² Aleecia M. McDonald and Lorrie Faith Cranor, ‘The Cost of Reading Privacy Policies’ (2009) 4 I/S: A Journal of Law and Policy for the Information Society 543, 563–564 <<http://www.is-journal.org/>> accessed 20 January 2016. If all Americans read privacy policies every time they visited a new website, it would take them 54 billion hours or on average 40 minutes a day, effectively reducing the time they browse the internet for shopping, playing games etc. They would also lose \$781 billion by way of the opportunity cost value of the time taken to read privacy policies.

⁴⁰³ Directive 95/46/EC Article 10; Directive 95/46/EC Article 11.

guidance on the presentation of the information, accessibility as well as provisions on protecting children's personal data.

The EU GDPR 2018 has expanded the transparency principle⁴⁰⁴ and it will apply throughout the life cycle of data processing. Equally important, it has for the first time; recognised the need to provide special guidance to protect children's digital privacy. Recital 38⁴⁰⁵ recognises that children may be less aware of the online privacy risks. Information should be in a clear and plain language⁴⁰⁶ so that it resonates with children and they can recognise the message directed to them.⁴⁰⁷

The EU GDPR 2018 does not define transparency but Recital 31⁴⁰⁸ defines it in the context of data processing as information that should be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, for any information addressed specifically to a child'.⁴⁰⁹ Communication of information to data subjects will comply with above elements.⁴¹⁰ The first three elements relevant for the purposes of this thesis will be discussed in the next section.

⁴⁰⁴ EU GDPR 2018 Recital 58 and Article 12 and 13. The Regulation requires controller to also furnish contact details of the data protection officer; the right to lodge a complaint with a supervisory authority; information about whether data is transferred to a third country; the legitimate interests pursued by the controller; and whether further processing will be required.

⁴⁰⁵ EU GDPR 2018.

⁴⁰⁶ EU GDPR 2018 Recital 58.

⁴⁰⁷ Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa 11 April 2018)

[file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018.

⁴⁰⁸ EU GDPR 2018.

⁴⁰⁹ EU GDPR 2018 Article 12.

⁴¹⁰ Ibid.

3.2.4.1. 'Concise, transparent, intelligible and easily accessible'⁴¹¹

Art29 WP clarifies 'concise and transparent' as information that is efficiently and succinctly presented to avoid information fatigue.⁴¹² It advises privacy policies to be layered for the data subject to navigate a section and immediately access the required information. This is beneficial for children because they can easily access information without having to go through the entire document.

Art29 WP defines 'intelligible' as information that can be understood by an average member of the audience.⁴¹³ It requires website operators/data controllers to have knowledge of the people they collect information from. Videogame website operators should draft privacy policies that are intelligible for children as their intended target audience.

'Easily accessible' means that privacy policies will be placed prominently using positioning and colour.⁴¹⁴ This is similar to provisions on prominence of privacy policies in the U.S. data privacy regime (*see 4.4 & 4.4.1*). The EU GDPR 2018 is attempting to treat children as a special class of data subjects so that they can easily locate and read privacy notices.

⁴¹¹ EU GDPR 2018 Recital 58 and Article 12(1).

⁴¹² Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa 11 April 2018)

[file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018

⁴¹³ Ibid.

⁴¹⁴ Ibid.

3.2.4.2. "Clear and plain language"⁴¹⁵

The EU GDPR 2018 has placed emphasis on the requirement for clear and plain language which is also referred to in Recital 42⁴¹⁶ as a pre-requisite for consent. Article 29 provides guidance that information should avoid complex and complicated sentences. It gives poor practice examples such as 'we may use your personal data for research purposes' where it is unclear what kind of 'research' this refers to.⁴¹⁷ The EU GDPR 2018 has emphasised transparency and realised that data subjects of all ages including children will be subject to data processing.

3.2.4.3. 'the requirement for clear and plain language is of particular importance when providing information to children'⁴¹⁸

Art29 WP gives specific guidance when providing information to children.⁴¹⁹ It gives the example of UN Convention on the Rights of the Child in Child Friendly Language⁴²⁰ which it states employs a child-centric language. This is helpful guidance but the lack of a specific standard for readability would result in website operators deriving their own interpretations for structuring children's privacy policy. It is recommended that following a set standard for readability that is targeted towards a certain age group will remove this uncertainty (*see 5.5.2.2; 6.2.2 & 6.4.1; 7.6*)

⁴¹⁵ EU GDPR 2018 Article 12(1).

⁴¹⁶ EU GDPR 2018.

⁴¹⁷ Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa 11 April 2018)

[file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018

⁴¹⁸ EU GDPR 2018 Article 12(1).

⁴¹⁹ Ibid.

⁴²⁰ <https://www.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf> accessed 21 May 2018.

The next section will discuss consent, which is one of the most fundamental principles of any data protection and privacy regime.

3.2.5. Consent

The concept of consent authenticates acts that would then be constituted legal.⁴²¹ For processing to be legitimate, one of the conditions under Article 7 of Directive 95/46/EC had to be met, namely unambiguous consent from the data subject,⁴²² and this was defined as ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’.⁴²³ Consent is one of the seven grounds for legitimate processing of data. In the absence of consent, the Directive still facilitated the data controller with other grounds that could then be relied on, to justify a wide range of processing.⁴²⁴

Directive 95/46/EC did not expressly define consent, so the European Commission and the Art29 WP attempted to provide instances of valid and invalid consent, focusing on elements such as unambiguous, specific and informed.⁴²⁵ So, for instance, consent was given ‘freely’ when was given without intimidation or deception,⁴²⁶ and ‘informed’ consent meant that the data subject had a clear understanding and

⁴²¹ Deryck Beyleveld and Roger Brownsword, *Consent in Law* (Hart Publishing 2007); Michael Birnhack, ‘Soft Legal Globalisation: The Role of the EU Data Protection Directive in the Emerging Global Data Protection Regime’ (2008) <<http://www.tau.ac.il/law/minerva2/Birnhack.pdf>> accessed 5 January 2016.

⁴²² Directive 95/46/EC Article 7(a).

⁴²³ Directive 95/46/EC Article 2(h); Consent is further categorised into explicit consent which is given for sensitive data. Directive 95/46/EC Article 8(2)(a). Consent is needed to ensure legitimacy of processing as well as transfer of data to third countries that do not possess adequate levels of protection Directive 95/46/EC Article 26(1)(a).

⁴²⁴ Article 29 EU Data Protection Working Party, ‘Opinion 15/2011 on the Definition of Consent’ (Europa, 13 July 2011) <http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=3&hl=en&ct=clnk&gl=uk> accessed 14 May 2016.

⁴²⁵ Ibid.

⁴²⁶ Ibid.

appreciation of the facts as well as implications of any actions taken.⁴²⁷ The e-Privacy Directive states in Recital 17 that consent can be given through any appropriate means as long as it is 'freely given, specific and informed indication of the user's wishes, including by ticking a box when visiting an internet website'.⁴²⁸

The understanding from existing guidance is that consent authorises the data subject to make conscious, rational and autonomous choices in relation to the processing of their personal data.⁴²⁹ But children are expected to consent to lengthy, complicated documents as terms of service and privacy policies before they can access the services of the website. Such consent is not informed and freely given.

3.2.5.1. The difficulty with consenting to privacy notices

There is an extraordinary amount of evidence collected by Yannis Bakos to suggest that consumers willingly sign all sorts of contractual agreements without reading them.⁴³⁰ The clicking without reading phenomenon found online is an exact replica of these findings. Bakos performed a pioneering study in the U.S. and found that across 120,545 observations of potential online buyers, only 55 accessed the EULAs (end user licence agreements) and surprisingly viewed them on average for only 47.7 seconds.⁴³¹ Quite significantly, data subjects are more likely to consent when presented with a consent request than anywhere else.⁴³² This presumably creates

⁴²⁷ Ibid.

⁴²⁸ Directive 2002/58/EC (n 14) Recital 17.

⁴²⁹ Bart W. Schermer, Bart Custers and Simone Van Der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics Info Technol 171.

⁴³⁰ Yannis Bakos, Florencia Marotta-Wurgler and David R. Tossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' (Jstor, 2014) <<https://webcache.googleusercontent.com/search?q=cache:HELW1FvT1j0J:https://www.journals.uchicago.edu/doi/abs/10.1086/674424+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 15 May 2016.

⁴³¹ Ibid.

⁴³² Noellie Brockdorff and Sandra Appleby-Arnold, 'What Consumers Think' [2013] EU consent project, Workpackages 7.

doubts as to the effectiveness and protection provided by consent. According to industry practice, data subjects are provided with an unreasonably long and complicated set of legal jargon in fine print, and the data subject is forced to consent to these terms. Such practices are hard to reconcile with children, who are avid users of the online community.

3.2.5.2. Children and the requirement to give valid consent

It is extremely important to protect children's digital privacy for several reasons. Firstly, children are vulnerable and may possess different levels of maturity in understanding privacy risks online.⁴³³

Children can disclose personal data about themselves and third parties to complete strangers, and the information can be abused and exploited by direct marketers to target vulnerable people.⁴³⁴ But the Directive grouped both children and adults under the combined term 'data subjects'.⁴³⁵

Since the Directive did not distinguish between children and adults, EU member states adopted different ages of discernment and practices in validating consent from children (see 3.1.2). Some websites in the EU, such as McDonald's,⁴³⁶ require parental consent by sending them a link on their email address to accept the registration. The

⁴³³ There are many agencies and centres such as the Child Exploitation and Online Protection Centre that are premised on the idea of advising and keeping children safe from internet-based exploitation. CEOP, 'CEOP: Child Exploitation & Online Protection Centre – Internet Safety' (NCA) <<https://ceop.police.uk/>> accessed 15 May 2016.

⁴³⁴ Rob Sumroy, 'Data Protection and Direct Marketing: Child's Play' (Slaughter and May, March 2006) <<https://www.slaughterandmay.com/media/39158/marketing%20part%203.pdf>> accessed 15 May 2016.

⁴³⁵ 'Opinion 2/2009 on the Protection of Children's Personal Data (Children's Guidelines and the Special Case of Schools)' (Europa. 2009) <http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=2&hl=en&ct=clnk&gl=uk> accessed 14 April 2018.

⁴³⁶ <<http://www.happystudio.com>>.

EU GDPR 2018 has for the first time recognised children as a special class of data subjects that need additional protection.⁴³⁷ Children under 16 years will be required to give parental consent. But the regulation allows member states to reduce the age to 13 years in accordance with their discretion. This can cause the same uncertainty that exists today in defining a child.

3.2.5.3. Are the current procedures for parental consent adequate?

There are difficulties around verifying consent for children under a certain age such as with a simple mouse-click. Requesting a parent's email address for registration poses numerous difficulties. Any email address can be given, and the registration process completed without the parent's involvement. Apart from requesting a parent's email address, the U.S. has introduced provisions to ban children's access to online material.⁴³⁸ Such robust measures can only do more harm as regulators lose track of opportunities that children can be provided with online, and therefore restraining children from a productive and enjoyable online experience.⁴³⁹

Eleni Kosta recognised that consent can provide a misleading understanding of protecting privacy.⁴⁴⁰ Jurists have recognised the periods, pre- and post-consent, that bring their own difficulties and uncertainties.

For instance, when is the actual requirement to give consent needed? Is it once, for the entire application, or on every click? What conditions need to be met to fulfil the need for valid consent? Is any prior information needed? What is the format needed

⁴³⁷ EU GDPR 2018 Article 8.

⁴³⁸ Ibid.

⁴³⁹ Ibid.

⁴⁴⁰ Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff 2013).

for consent? Does it always have to be explicit or can it be implied as well? How can consent be verified etc?⁴⁴¹

3.2.5.4. Definition of ‘unambiguous consent’ needs clarity

The Art29 WP provided guidance that ‘unambiguous consent’ should constitute a positive act such as signing a contract between the data controller and data subject before the transfer takes place.⁴⁴² In most cases of transborder data flows, there is no direct contact between data controllers and data subjects. The controller has to prove that consent was actually obtained, and the transfer was based on provision of sufficient information including the fact that there is inadequate protection in the third country.⁴⁴³ It also has to be noted that, once the transfer of data takes place, it is not possible for data subjects to assert their rights if they are breached. Binding corporate rules⁴⁴⁴ may perhaps tie up both employees and the company and guarantee that data subjects can bring a claim against the company if their rights are breached.⁴⁴⁵

⁴⁴¹ Liam Curren and Jane Kaye, ‘Revoking Consent: A ‘Blind Spot’ in Data Protection Law?’ (2010) 26(3) *Computer Law and Security Review: The International Journal of Technology and Practice* 273, 273–283.

⁴⁴² Binding corporate rules allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide an adequate level of protection. Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (Europa, 2005) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf> accessed 17 January 2016.

⁴⁴³ Eleni Kosta, *Consent in European Data Protection Law* 233–234 (Martinus Nijhoff 2013); Victoria Hordern, ‘Consent – the Silver Bullet’ (2013) <<http://www.fieldfisher.com/publications/2013/02/consent-the-silver-bullet>> accessed 16 January 2016.

⁴⁴⁴ Article 29 EU Data Protection Working Party, ‘Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995’ (Europa, 2005) <www.pdpjournals.com/docs/88080> accessed 16 January 2016. Under the EU GDPR 2018, binding corporate rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a member state for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. EU GDPR 2018 Article 4(20).

⁴⁴⁵ Olivier Proust and Emmanuelle Bartoli, ‘Binding Corporate Rules: A Global Solution for International Data Transfers’ (2012) 2(1) *International Data Privacy Law* 35, 36.

3.2.5.5. EU GDPR 2018 on the ‘definition for consent’

The EU GDPR 2018 requires consent in the context of a written declaration.⁴⁴⁶ It should be easy to withdraw consent as it is to give.⁴⁴⁷ This means that websites cannot imply consent anymore. Cookies and similar technologies that collect personal data cannot apply automatically.⁴⁴⁸ Individuals will have to be provided with an opt-out button to withdraw consent as well as an opt-in button if they decide to change their preference. But this can cause some unwanted consequences such as consent fatigue from repeated consent messages for website visitors.⁴⁴⁹ It can lead to ‘consent transaction overload’,⁴⁵⁰ diminishing its effectiveness.

EU GDPR 2018 also makes a distinction between ‘unambiguous consent’ which is required for non-sensitive data,⁴⁵¹ and ‘explicit consent’ which is required for sensitive data.⁴⁵² The distinction between the two terms creates a confusion because consent is still consent whether given unambiguously or explicitly. It is an affirmative action agreeing to the processing of personal data. Explicit consent is given when a user ticks a box (hence an explicit affirmative action). An example of giving unambiguous consent is discussing one’s ailment with a doctor. There is an implied

⁴⁴⁶ EU GDPR 2018 Article 7(2).

⁴⁴⁷ EU GDPR 2018 Article 7(3).

⁴⁴⁸ EU GDPR 2018 Recital 30; Cookies and GDPR: what you need to know (Automated Intelligence 4 December 2017) < <https://www.automated-intelligence.com/news-and-events/blog/cookies-gdpr-need-know/> > accessed 21 May 2018.

⁴⁴⁹ Christine Jolls and Cass R. Sunstein, ‘Debiasing through Law’ (2006) 35(1) *The Journal of Legal Studies* 199, 212.

⁴⁵⁰ Bart W. Schermer, Bart Custers and Simone Van Der Hof, ‘The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection’ (2014) 16(2) *Ethics Info Technol* 171, 176–178.

⁴⁵¹ EU GDPR 2018 Articles 4 and 6.

⁴⁵² EU GDPR 2018 Articles 9(2)(a).

understanding that the content of discussion will remain confidential with the doctor (consent is unambiguous and implied, but not explicit).⁴⁵³

3.2.5.6. EU GDPR 2018 on the requirement of children giving consent

Children need additional protection online.⁴⁵⁴ The European Commission therefore introduced the concept of parental consent when processing the personal data of children under the age of 13 years and offering them information society services.⁴⁵⁵ An information society service was described in Article 1(2) of Directive 98/34/EC⁴⁵⁶ (amended by Directive 98/48/EC)⁴⁵⁷ as ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’. Upon closer inspection, this definition will most likely attract wide implications and apply to any kind of commercial website.

3.2.5.7. EU GDPR 2018 on ‘parental consent mechanism’ and the term ‘verifiable’

The EU GDPR 2018 authorises parental consent but falls short of providing the process of parental consent mechanism.⁴⁵⁸ The data controller will verify consent, taking into consideration existing technology.⁴⁵⁹ The EU GDPR 2018 does not provide

⁴⁵³ Phil Lee, ‘The ambiguity of unambiguous consent under the GDPR’ (fieldfisher 7 June 2016) <<https://privacylawblog.fieldfisher.com/2016/the-ambiguity-of-unambiguous-consent-under-the-gdpr>> accessed 20 May 2018.

⁴⁵⁴ Lina Jasmontaite and Paul De Hert, ‘The EU, Children under 13 years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet’ (2015) 5(1) IDPL 20, 20–33.

⁴⁵⁵ EU GDPR 2018 Article 8(1).

⁴⁵⁶ Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations.

⁴⁵⁷ Directive 98/48/EC of the European Parliament and of the European Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

⁴⁵⁸ Luke Danagher, ‘An Assessment of the Draft Data Protection Regulation: Does It Effectively Protect Data?’ (2012) 3(3) European Journal of Law and Technology.

⁴⁵⁹ EU GDPR 2018 Article 8(2).

any guidance on what ‘verifiable’ means. The European Commission advises that delegated acts will be employed to ‘provide the criteria and requirements for the methods to obtain verifiable consent’.⁴⁶⁰

The EU GDPR 2018 invalidates consent if there is a significant difference between the data subject and data controller. When data subjects want to access a website such as news or a clothing shop, they will be presented with a consent request. At this point, they don’t really have a choice but to accept it. There is no room for negotiation but either consent will be given, and services will remain effective or the data subject will have to leave the website entirely.

Explicit consent does not form part of the definition of consent.⁴⁶¹ But it will fall under the clear affirmative action required by the unambiguous indication of one’s wishes.⁴⁶² Since cookies already require an opt-in, how do the new rules on explicit consent make changes?⁴⁶³ The strict consent measures could affect direct advertising since they would no longer be able to target customers directly, causing loss of revenues that could discourage innovation and dynamism in the industry.

The next section will consider the rules for transferring data from EU to third countries outside the EU.

⁴⁶⁰ EU GDPR 2018 Article 8(3); Children’s Data Protection and Parental Consent: A Best Practice Analysis to Inform the EU Data Protection Reform (Advertising Education Forum, 2013) 5 <<http://www.aeforum.org/gallery/5248813.pdf>> accessed 20 January 2016.

⁴⁶¹ EU GDPR 2018 Article 4 ‘Defintions’ and Recital 32

⁴⁶² GDPR consent guidance (ICO) < <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/>> accessed 19 May 2018.

⁴⁶³ Damian Clifford, ‘EU Data Protection Law and Targeted Advertisement: Consent and the Cookie Monster – Tracking the Crumbs of Online User Behavior’ (2014) 5(3) JIPITEC 194 <<http://www.jipitec.eu/issues/jipitec-5-3-2014/4095>> accessed 12 December 2015.

3.2.6. Transfer of data to third countries

Articles 25 and 26⁴⁶⁴ provide rules for the transfer of personal data from EU member states to countries outside the EU. On 26 July 2000, the Commission adopted Decision 520/2000/EC⁴⁶⁵ (the 'Safe Harbour Principles'). U.S. organisations will have to comply with the Safe Harbour Principles to ensure that data transferred from the EU to the U.S. is given adequate protection in accordance with the principles of the earlier Directive 95/46/EC⁴⁶⁶ and the EU GDPR 2018 which is now in force.⁴⁶⁷

In the *Schrems* case, Facebook's practice in transferring personal data of its European subscribers to servers located in the U.S. was questioned.⁴⁶⁸ The court had to consider the validity of the Safe Harbour Privacy Principles in protecting the data that was transferred from the EU to the U.S. It was found that the scheme enabled interference by the U.S. public authorities with the fundamental principles of individuals⁴⁶⁹ and the U.S. did not adopt rules to limit any such interference.⁴⁷⁰ The data was processed in an incompatible manner and for purposes that were strictly beyond the purposes for which it was necessary and proportionate to the protection

⁴⁶⁴ Data Protection Directive 95/46/EC.

⁴⁶⁵ Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related FAQ issued by the US Department of Commerce (Europa, 2004) <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf> accessed 15 April 2016.

⁴⁶⁶ European Commission, 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (Europa, 2013) <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf> accessed 11 April 2016.

⁴⁶⁷ EU GDPR 2018 Chapter V Articles 44,45 & 46.

⁴⁶⁸ *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14).

⁴⁶⁹ Court of Justice of the European Union, 2015. 'The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid' (Europa) <http://curia.europa.eu/jcms/jcms/P_180250/> accessed 11 April 2016

⁴⁷⁰ *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14), [87], [88].

of national security.⁴⁷¹ Therefore, the court invalidated the Safe Harbour Privacy Principles on 6 October 2015.⁴⁷²

To ensure continued safety of transferring personal data from EU member states to the U.S., the EU–U.S. Privacy Shield between the European Commission and Department of Commerce was announced to replace the Safe Harbour Framework.⁴⁷³ This framework reflects the decision of the ECJ in the *Schrems* case.⁴⁷⁴ It involves strong obligations on companies, greater transparency and a new redress and complaint resolution mechanism for EU citizens.⁴⁷⁵ Microsoft has hailed the new framework as an important step in enhancing trust in the digital economy.⁴⁷⁶

On 30 May 2016, the European Data Protection Supervisor (EDPS) raised concerns that the Privacy Shield was not robust enough for future legal scrutiny by the ECJ.⁴⁷⁷ In April 2016, the Art29 WP issued an opinion requesting clarification on a number of issues such as the principle of data retention (the continued storage of an organisation’s data for compliance or business reasons)⁴⁷⁸ and the application of the purpose limitation principle (personal data must be collected for ‘specified, explicit and legitimate’ purposes (purpose specification) and not be ‘further processed in a

⁴⁷¹ Ibid 90.

⁴⁷² *Judgment in Case C-362/14 Maximilian Schrems v Data Protection Commissioner*.

⁴⁷³ The EU-U.S Privacy Shield (ITIC 2016) <<http://www.itic.org/safeharbor>> accessed 11 April 2016.

⁴⁷⁴ European Commission, ‘Restoring Trust in Transatlantic Data Flows through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield’ (Europa, 2016) <http://Europa.eu/rapid/press-release_IP-16-433_en.htm> accessed 12 April 2016.

⁴⁷⁵ Ibid.

⁴⁷⁶ John Frank, ‘Microsoft’s Commitments, including DPA Cooperation, under the EU-U.S. Privacy Shield’ (Microsoft, 2016) <<https://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/>> accessed 12 April 2016.

⁴⁷⁷ European Data Protection Supervisor ‘Privacy Shield: More Robust and Sustainable Solution Needed’ (Europa, 30 May 2016) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 14 March 2017.

⁴⁷⁸ ‘Data Retention’ (TechTarget February 2014) <<https://searchstorage.techtarget.com/definition/data-retention>> accessed 21 September 2017.

way incompatible' with those purposes (compatible use)⁴⁷⁹ to the processing of data, which has not been clearly agreed to between the EU and the U.S. in the Privacy Shield.⁴⁸⁰

The EDPS, Giovanni Buttarelli, conceded that if the purposes for which exceptions allow access to the personal data of European citizens are the same as in the Safe Harbour Framework, this would be a repeat of the same instances that invalidated the previous framework.⁴⁸¹

The proposed system favour accountability and transparency, but there are some concerns that need to be addressed. Processors will have to renegotiate contractual arrangements or else they risk non-compliance.⁴⁸² At present, the EU GDPR 2018 does not provide any guidance on how this will happen, and businesses remain in the dark. Information is needed in the form of guidance by the Art29 WP and the recitals, otherwise businesses complying with the EU GDPR 2018 will involuntarily be in breach of the law, which will create an atmosphere of confusion, mistrust and demoralisation.

The previous sections dealt with the principles related to the definition of personal data, collection and processing, principles of consent and transfer of personal data to

⁴⁷⁹ Article 29 EU Data Protection Working Party, 'Opinion on 3/2013 on Purpose Limitation' (Europa, 2 April 2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 21 September 2017.

⁴⁸⁰ Article 29 EU Data Protection Working Party, 'Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision' (Europa 13 April 2016) <<http://www.pdpjournals.com/docs/88536.pdf>> accessed 14 March 2017.

⁴⁸¹ European Data Protection Supervisor, 'Privacy Shield: More Robust and Sustainable Solution Needed' (Europa, 30 May 2016) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 28 March 2017.

⁴⁸² 'Data Protection and Service Providers – New Obligations, Liabilities and Contract Changes Loom' (Out-Law.com, 2015) <<http://www.out-law.com/en/articles/2015/september/data-protection-and-service-providers--new-obligations-liabilities-and-contract-changes-loom/>> accessed 14 December 2015.

third countries. The following sections will consider the rights that data subjects are entitled to.

3.2.7. Rights of data subjects under the Directive 95/46/EC

3.2.7.1. Data subject's right to object

Under the repealed Directive 95/46/EC, data subjects were allowed the right to object to processing of their data on 'compelling legitimate grounds'.⁴⁸³ The EU GDPR 2018 stipulates that 'Further processing ... shall be lawful if these interests override the interests of the data subject'.⁴⁸⁴ If the data subject objects, the controller will have to prove 'compelling legitimate grounds' for continuing the processing, or that the processing is necessary in connection with his legal rights, to override the interests of the data subject.⁴⁸⁵ Under Recital 65 EU GDPR, the right to be forgotten is not only crystallised into law but is greatly relevant when the data subject is a child. This will create problems if the organisation relies on its own legitimate interests as a justification for processing personal data. So, rather than minimising the broad implications of legitimate interests, the EU GDPR 2018 encourages a 'non-excessive' data processing regime. Data subjects will find it difficult to challenge acts they have little knowledge of.

EU lawmakers should curtail the importance attached to the term 'legitimate interests' or provide additional guidance on its meaning, form and extent. Recitals could be provided that show instances of what amounts to 'legitimate interests'.

⁴⁸³ Directive 95/46/EC Article 14(a).

⁴⁸⁴ EU GDPR 2018 Article 6(4).

⁴⁸⁵ EU GDPR 2018 Article 19.

3.2.7.2. Individual participation principle

Article 12 of Directive 95/46/EC provided the right of access, which allowed data subjects the right to obtain from the data controller, communication, in an intelligible form, that data is undergoing processing.⁴⁸⁶ Data subjects also have the right to rectify, erase or block processing of their data⁴⁸⁷ if it is inaccurate and does not comply with the provisions of the earlier Directive.⁴⁸⁸

Advocate General Sharpston admitted that the Directive did not establish a right of access to a document which contains personal data, nor was there a specific form in which the data will be made accessible.⁴⁸⁹ She equated right of access to the fundamental right to protection of privacy.⁴⁹⁰ But the ECJ adopted a very wide interpretation⁴⁹¹ and only dealt with the fundamental right to protection of personal data rather than protection of privacy as well.⁴⁹²

The European Commission has been adamant that data subjects should possess sufficient control over their own data for effective data protection.⁴⁹³ The right to

⁴⁸⁶ *Heinz Huber v Bundesrepublik Deutschland* (2008) Case C-524/06; OECD Guidelines on the protection of privacy and transborder flows of personal data (OECD, 2013). <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>> accessed 17 December 2015.

⁴⁸⁷ Directive 95/46/EC Article 12.

⁴⁸⁸ Bart Van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4(4) IDPL 307, 314.

⁴⁸⁹ Opinion of Advocate General Sharpston delivered on 12 December 2013. *YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel (C-372/12) v M and S*, [93(3)].

⁴⁹⁰ *Ibid* 60.

⁴⁹¹ Xavier Tracol, 'Back to Basics: The European Court of Justice Further Defined the Concept of Personal Data and the Scope of the Right of Data Subjects to Access It' (2015) 31(1) CLSRev 112, 115.

⁴⁹² *YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel (C-372/12) v M and S*, [42].

⁴⁹³ 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the

access is encapsulated in Article 15 of the EU GDPR 2018, but additional elements such as the right to be informed about the storage period and the right to rectification, erasure and lodge a complaint have also been included.⁴⁹⁴ Additionally, individuals will also have a right to data portability,⁴⁹⁵ which allows individuals to obtain and easily transfer their personal data between different service providers.⁴⁹⁶

Smart tracking technologies like cookies are installed on the user's device when they visit a website. Privacy notices should detail the use of tracking technologies by the website and the methods to disable them. The next section will consider the e-Privacy Directive, which regulates use of cookies as data tracking mechanisms, and the changes contained within the EU GDPR 2018.

3.3. e-Privacy Directive (the EU Cookie Directive)

The e-Privacy Directive is a continuation of the efforts undertaken by the earlier Directive 95/46/EC to strengthen data protection and privacy in the digital age. It was introduced by the European Commission to regulate how companies collect individuals' data online and allow online users greater choice over how cookies are used to track them.⁴⁹⁷

European Union' (European Commission, 2010) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609>> accessed 20 December 2015.

⁴⁹⁴ EU GDPR 2018 Articles 13 – 15.

⁴⁹⁵ EU GDPR 2018 Article 20; 'The Right to Data Portability' (ICO) <<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/>> accessed 21 September 2017.

⁴⁹⁶ 'Stronger Data Protection Rules for Europe: the EU Adopts the Data Protection Reform Package' (Europa, 2015) <[http://Europa.eu/rapid/press-release MEMO-15-6385_en.htm](http://Europa.eu/rapid/press-release_MEMO-15-6385_en.htm)> accessed 28 December 2015.

⁴⁹⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

The e-Privacy Directive will be replaced with the new EU e-Privacy Regulation⁴⁹⁸ which aims to reinforce trust and security in the EU by updating the legal framework on electronic communication.⁴⁹⁹ Since the EU has reformed its data protection framework with the EU GDPR 2018, the e-Privacy Regulation will be adapted to align with these new rules.⁵⁰⁰ Since it is a regulation, like the EU GDPR 2018, it will be applicable across EU member states without formal legislative adoption. One of the changes it stipulates is to make cookie consent more user friendly. This means it will remove cookie consent pop-ups, as browser settings will provide for an easy way to accept or refuse tracking cookies and other identifiers. The proposal also bans unsolicited electronic communications by emails.⁵⁰¹

This is a positive change in terms of treating children as a special class of data subjects. They can easily alter their browser settings and change their privacy without having to consult complicated browser documentation. By doing so, they can exert more informed control over their privacy settings.

3.3.1. Smart tracking technologies: cookies

Cookies assist in synchronising remote website servers and users' browsers to display the full length of features offered.⁵⁰² Cookies are programming techniques that can be utilised by web developers to store and retrieve data about users.⁵⁰³ They facilitate

⁴⁹⁸ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

⁴⁹⁹ Proposal for an ePrivacy Regulation (europa) < <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>> accessed 24 June 2018.

⁵⁰⁰ Ibid.

⁵⁰¹ Ibid.

⁵⁰² 'Privacy Concerns on Cookies' <<http://www.allaboutcookies.org/privacy-concerns/>> accessed 20 January 2016.

⁵⁰³ 'What Are Cookies?' (1998) 5(8) Inside the Internet.

automatic logins and authentication, remembering user preferences, shopping cart functionalities, third-party ad serving, ad management etc.⁵⁰⁴ Cookies can be session-based or temporary files. Some of them can stay in the browser from a few days to a couple of months. Cookies can be first-party, which improve online experience and help visitors stay logged on. Third-party cookies track activity and recognise frequent and returning visitors as well.⁵⁰⁵

On the face of it, cookies seem harmless but, upon closer inspection, cookies store users' personal data and distribute this information without their knowledge. It is feared that, no matter how hard we try, we always tend to leave a trail of cookie crumbs, making it possible for the trail to lead back to us.⁵⁰⁶

3.3.2. The difficulty with managing cookies

Previously, under Article 5(3) of the e-Privacy Directive, cookies were allowed only if the website user had been 'provided with clear and comprehensive information ... about the purposes of processing and offered the right to refuse such processing by the data controller'. This was an informed opt-out approach.⁵⁰⁷ However, this Article has been amended by the e-Privacy Amendment Directive⁵⁰⁸ and now not only will the website operator be required to inform visitors that cookies will be downloaded

⁵⁰⁴ 'Privacy Concerns on Cookies' <<http://www.allaboutcookies.org/privacy-concerns/>> accessed 20 January 2016.

⁵⁰⁵ John Barnes, 'Internet Users' Privacy Concerns May Mean Cookies Start to Crumble' *The Guardian* (24 May 2013) <<http://www.theguardian.com/technology/blog/2013/may/24/internet-privacy-cookies-firefox>> accessed 27 January 2016.

⁵⁰⁶ 'Cookies: Leaving a Trail on the Web' (i.t.pie) <<http://www.itpie.co.uk/blog/cookies-leaving-a-trail-on-the-web>> accessed 26 April 2018.

⁵⁰⁷ Robert Bond, 'The EU E-Privacy Directive and Consent to Cookies' [2012] 68(1) *The Business Lawyer*.

⁵⁰⁸ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection law.

onto their computer but, additionally, prior consent will be needed, to which there must be both an 'opt-in' and an 'opt-out' mechanism.⁵⁰⁹

The difficulty created is when managing cookie settings. Recital 66 of the e-Privacy Amendment Directive provides that consent can be obtained through the appropriate browser settings. The drawback is that it is site-specific, which means it will only block the cookies on a specific server and will not block cookies on other websites. For generalised blocking, one should manage their cookies via their browser's cookie settings. Different browsers offer different ways to configure one's browser's cookie settings. This might seem onerous and unimportant to a child. The Department for Culture, Media and Sport conducted research into the potential impact of cookie regulation⁵¹⁰ and found that 37% of adults are unaware about how to manage cookies.

3.3.3. Flash cookies

Flash cookies are different to standard HTTP cookies⁵¹¹ and pose a further problem. Since they are not controlled by the browser and are stored in a location different to HTTP cookies, flash cookies will not expire, the user will not know which files they are contained in to access them and deleting browsing history will not affect them.⁵¹²

⁵⁰⁹ UK Information Commissioner's advice on the use of cookies and similar technologies for storing information under the new rules (ICO, May 2012) <https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf> accessed 20 January 2016.

⁵¹⁰ David Lancefield, The Department for Culture, Media and Sport Research into consumer understanding and management of internet cookies and the potential impact of the UK Electronic Communications Framework (Department for Culture, Media and Sport) <http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf> accessed 23rd January 2016.

⁵¹¹ 'HTTP Cookies' <<https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>> accessed 13 April 2018. An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser that recognises the user.

⁵¹² Ashkan Soltani, 'Flash Cookies and Privacy' (AshkanSoltani 2009) <<http://ashkansoltani.org/2009/08/09/flash-cookies-and-privacy/>> accessed 20 January 2016.

Such technological advancements in cookies pose new found risks to privacy online because it defeats the purpose of browser settings to obtain valid and informed consent.

The amended e-Privacy Directive has endeavoured to expand the law on cookies but lacks guidance on how consent will be given or obtained.⁵¹³ Browser solutions are still under operation, with several member states considering them as a solution to consent.⁵¹⁴

As a result, many European states took different approaches,⁵¹⁵ with some complying with the earlier Directive whereas others concluded that their current laws were sufficiently compatible.⁵¹⁶

In relation to children, the Art29 WP agreed that consent should be provided by parents; therefore, ad network providers should supply a notice to parents about the collection and use of children's information.⁵¹⁷ But, owing to the vulnerability of children, the Art29 WP unanimously agreed that advertisement providers should not target or influence children for purposes of behavioural advertising to begin with.⁵¹⁸

⁵¹³ Robert Bond, The EU E-Privacy Directive and Consent to Cookies [2012] 68(1) The Business Lawyer, 215–223.

⁵¹⁴ Ibid.

⁵¹⁵ Ibid.

⁵¹⁶ 'Opinion 15/2011 on the Definition of Consent' (Europa, 2011)

<http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=3&hl=en&ct=clnk&gl=uk> accessed 24 January 2016.

⁵¹⁷ 'Opinion 2/2010 Online Behavioural Advertising' (Europa, 2010)

<https://webcache.googleusercontent.com/search?q=cache:J1qvDBpz-SgJ:https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/junio/WP171en.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 22 January 2016.

⁵¹⁸ Ibid.

3.3.4. EU GDPR 2018 on the 'definition of cookies'

There is widespread criticism against the mysterious workings of the rather innocently named text file called 'cookie'. The implementation is erratic across European member states, resulting in uncertain and minimalistic enforcement action. Many view cookies have not benefitted users in relation to their privacy.⁵¹⁹ The EU GDPR 2018 requires a request for consent to process personal data to be provided in a clearly distinguishable, intelligible and easily accessible form,⁵²⁰ as such websites need to clearly define the different tracking methods used. Websites should inform users about the cookies that are necessary for the functioning of the website, that do not collect personal data and do not require consent.

Cookies used for analytics are not mandatory but facilitate a website's functionality. They are still clever ways to gather user's data and should not be imposed upon the user. Therefore, a user should be given the choice to opt-out.⁵²¹ Similarly, third-party cookies are also optional, and the user should be allowed to decide whether to opt-out. Further, the EU GDPR 2018 also provides that it must be as easy to withdraw consent as it is to give it.⁵²² If users choose to opt-out on one occasion, they should be given the option to opt-in when later their preferences change. The EU GDPR 2018 does not clarify the instances when users will need to opt-out once they have opted-in. And more importantly, how and why will children exercise this option.

⁵¹⁹ Richard Beaumont, 'Cookie Law Reform in 2016' (Optanon Privacy Matters. 2016) <<https://www.cookie-law.org/blog/2015/2/10/cookie-law-reform-in-2016/>> accessed 30 January 2016.

⁵²⁰ EU GDPR 2018 Article 7 and Recital 42.

⁵²¹ Cookies consent under the GDPR (EU GDPR Compliant) <<https://eugdprcompliant.com/cookies-consent-gdpr/>> accessed 18 May 2018.

⁵²² EU GDPR 2018 Article 7(3).

Having reviewed the impact of cookies under the EU GDPR 2018 through the lens of children as a special class of data subjects, cookie consent is a positive action. Children will be able to exercise the opt-in or opt-out button to reveal their preferences. It is unclear why children would want to opt-out of cookies once they have provided consent.

3.4. Conclusions

Directive 95/46/EC was a concerted effort by the EU to draft a comprehensive set of data privacy law that aimed to explain concepts such as personal data and consent, which can be integral parts of any data privacy framework.

There is little guidance on websites' data handling practices that data controllers should furnish users with. Since the Directive did not treat children as a special class of data subjects, it lacked guidance on the information that should be provided to children when collecting, processing and sharing their data. The EU GDPR 2018 does recognise the need to protect children (*EU GDPR Recital 38; see 1.1.1*). It has for the first time recognised that children may be less aware of online privacy risks⁵²³ and information regarding processing of children's data should be presented in clear and plain language that children can easily understand.⁵²⁴ But it lacks sufficient guidance on the standard of readability and information that should be provided to them in privacy policies.

The Directive catered to the 'purpose specification' principle and the 'principle of minimality', whereby data should be collected for specified, compatible and

⁵²³ EU GDPR 2018 Recital 38.

⁵²⁴ EU GDPR 2018 Recital 58.

legitimate purposes. However, terms such as ‘legitimate’ can be interpreted broadly and the data controller can be allowed to collect extensive information based on legitimate interests. This can abrogate the above principles and put children’s privacy at risk because they can be subject to extensive data collection practices.

The EU GDPR 2018 lacks provisions which guide website operators on the level of information they can collect from child users. Words such as ‘legitimate interests’ should be avoided. Rules should be drafted to ensure that data controllers only collect information for specified and very relevant purposes.

The EU GDPR 2018 requires information given to data subjects⁵²⁵ to be ‘concise, transparent, intelligible and easily accessible form, using clear and plain language, for any information addressed specifically to a child’.⁵²⁶ This provision can pave the way for introducing privacy policies specifically designed for children. The provision should also contain guidance on the standard for readability.

Articles 25 and 26 of Directive 95/46/EC required when data is transferred from EU to third countries the latter should have adequate safety standards that comply with the provisions of the Directive. The annulment of the Safe Harbour Principles⁵²⁷ resulted in the EU–U.S. Privacy Shield.⁵²⁸ The Directive lacked guidance on the rules such as who will supervise the observance of these rules, whether it is compulsory to comply with such requirements and who it applies to. The uncertainty attracted criticism from higher authorities. Legislators should review the validity and

⁵²⁵ EU GDPR 2018 Articles 12, 13 and 14

⁵²⁶ EU GDPR 2018 Article 12(1)

⁵²⁷ *Judgment in Case C-362/14 Maximilian Schrems v Data Protection Commissioner*; Court of Justice of the European Union, 2015. ‘The Court of Justice Declares that the Commission’s US Safe Harbour Decision Is Invalid’ (Europa) <http://curia.europa.eu/jcms/jcms/P_180250/> accessed 11 April 2016.

⁵²⁸ ‘The EU-U.S. Privacy Shield’ (ITIC, 2016) <<http://www.itic.org/safeharbor>> accessed 11 April 2016.

effectiveness of privacy frameworks that protect transfer of personal data. More importantly, how do such frameworks ensure data privacy for children?

The law does not provide guidance on the information that should be presented to children to facilitate their understanding of the websites data handling practices. Such requirements become even more demanding when the data subject is a child under 18 years of age. Children between the ages of 16 - 17 may exhibit limited understanding of the law (*see 5.5.2.4*) and the website's data handling practices. For them to read, understand and consent to the privacy policies, they should be able to understand what they read. The EU GDPR 2018 has made changes by introducing provisions that specifically relate to children. However, additional guidance is needed to regulate the relationship that website operators have with child data subjects through their use of online websites.

This chapter has explained the main principles of Directive 95/46/EC and the EU GDPR 2018 that deals with data handling practices contained in the privacy policy of a website.

The next chapter will discuss the main data protection and privacy laws in the U.S. and Canada that regulate the data handling practices of an online website privacy policy. This discussion will provide a rich understanding for the comparative analysis between the data privacy laws of the EU, the U.S. and Canada.

CHAPTER FOUR

DATA PROTECTION AND PRIVACY FRAMEWORK IN THE U.S. AND CANADA

4.1. Introduction

Chapter 3 evaluated the main principles of Directive 95/46/EC for processing personal data and the changes contained within EU GDPR 2018. This chapter discusses the data privacy frameworks in the U.S. and Canada that affect the digital privacy of users.

4.2. Comparative law methodology

This thesis evaluates the U.S. data privacy laws because six out of 10 videogames selected for the multiple case study are governed by U.S. laws (*Chapter 5 Table 5*). The U.S. represents one of the largest markets for the online gaming industry (*Chapter 5 Section 5.3.1.1*) It is an English-speaking legal system subject to democratic controls.

Playing videogames is the second highest online activity carried out by children between the ages of nine and 16 years (83%).⁵²⁹ Does the largest videogame jurisdiction (the U.S.) protect the digital privacy of children as one of the biggest online user communities?

⁵²⁹ Sonia Livingstone and others, 'Risks and Safety for Children on the Internet: the UK report' (The London School of Economics and Political Science, December 2010) <[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/National%20reports/UKReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf)> accessed 17 November 2017.

The U.S. has enacted laws that treat children as a special class of data subjects. The EU GDPR 2018 was partially inspired by the Children's Online Privacy Protection Act 1998 (COPPA).⁵³⁰ The U.S. experience can inform the debate about the adequacy of EU and Canadian data privacy law over the new data protection challenges related to children's ability to read, understand and consent to website's data handling practices.

This comparative analysis will lay down important guidelines to compare against the findings of the multiple case study. The comparison will determine whether privacy policies remain compatible with the governing law; additionally, whether the practice of privacy policies and the governing law remain compatible with the expectations for children to read, understand and consent to privacy policies.

In the U.S., COPPA regulates the data handling practices of websites directed to children under 13 years of age. In the U.S., states can promulgate their own data privacy laws, which can operate alongside federal laws like COPPA. The U.S. videogame websites selected for this study are also governed by the data privacy laws of California, Washington and Delaware, which will also be explored.

Canada is one of the biggest contributors to the videogame industry. Data privacy is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA), which will be analysed as part of the comparative analysis. The jurisdiction of Canada is selected because the literature review for this thesis is based significantly

⁵³⁰ Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) Information & Communications Technology Law 146.

on Canadian lecturer Sara Grimes's multiple case study of the data privacy issues resulting from data mining⁵³¹ practices in children's videogames.⁵³²

Section 4.3 briefly discusses the origins of data privacy law: the U.S. Constitution and case law. This section considers the role of the Federal Trade Commission and federal laws to protect children's digital privacy.

Sections 4.4–4.6 discusses sector-specific laws including the California Online Privacy Protection Act ('CalOPPA'), the Delaware Online Privacy Protection Act ('DOPPA') and Washington State privacy laws. A brief discussion occurs in Section 4.7 regarding the Fair-Trade Practices, which regulate the relationship between entities and businesses regarding data handling practices and have been adopted into various data privacy laws.

Section 4.8 deals with PIPEDA, which is the main data privacy law in Canada. Section 4.10 presents key findings of the comparative legislative analysis carried out in *Chapters 3 and 4*. Section 4.11 provides a conclusion for *Chapter 4* by threading the findings into the current thesis and introduce the next chapter.

4.3. Regulation of data protection in the U.S.

As opposed to its European counterparts, where the EU GDPR 2018 determines the collection, processing and use of personal data, the U.S. does not have a single piece

⁵³¹ Data mining is a process of extraction of useful information and patterns from huge data. It is also called the knowledge discovery process, knowledge mining from data, knowledge extraction or data/pattern analysis. Bharati M. Ramageri, *Data Mining Techniques and Applications* (2010) 1(4) IJCA.

⁵³² Grace Chung and Sara M. Grimes, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2005) 30(4) *Canadian Journal of Communication*.

of legislation that governs its data privacy framework.⁵³³ Instead, the U.S. regulates by industry and on a sector-by-sector basis. It derives data protection and privacy laws from numerous sources, including constitutional interpretations provided by courts, international agreements, several statutory laws and executive orders.⁵³⁴

The U.S. Constitution⁵³⁵ does not contain any right to privacy but the United States Bill of Rights⁵³⁶ protects certain features of privacy.⁵³⁷ The Fourth Amendment ensures the ‘right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures’.

4.3.1. Cases that shaped the right to privacy in the U.S.

One of the earliest cases that recognised an individual’s right to privacy was *Boyd v United States*, where the United States Supreme Court unanimously agreed that a search and seizure could fall within the meaning of the Fourth Amendment.⁵³⁸

*Laird v Tatum*⁵³⁹ was one of the earliest cases that raised issues relating to the legitimate use of computerised personal information systems⁵⁴⁰ and its adverse effect on the rights contained in the First Amendment.⁵⁴¹

⁵³³ Robert Hasty, Trevor W. Nagel and Mariam Subjally White and Case, ‘Data Protection Law in the USA’ (A4ID, August 2013) <https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf> accessed 20 June 2016.

⁵³⁴ Jean Slemmons Stratford and Juri Stratford, ‘Data Protection and Privacy in the United States and Europe’ (IAassist, 1998) <<http://www.iassistdata.org/sites/default/files/iqvol223stratford.pdf>> accessed 20 June 2016

⁵³⁵ <<http://constitutionus.com/>> accessed 20 June 2016.

⁵³⁶ <https://www.aclu.org/united-states-bill-rights-first-10-amendments-constitution> accessed 20 June 2016.

⁵³⁷ Ibid.

⁵³⁸ *Boyd v United States* 116 U.S. 616 (1886) 634, 635; *Meyer v Nebraska*, 262 U.S. 390 (1923); *Pierce v Society of Sisters*, 268 U.S. 510 (1925); *Pierce v Society of Sisters*, 268 U.S. 510 (1925); *Griswold v Connecticut*, 381 U.S. 479 (1965); *Roe v Wade*, 410 U.S. 113 (1973).

⁵³⁹ *Laird v Tatum*, 408 U.S. 1 (1972).

⁵⁴⁰ U.S. Congress, Office of Technology Assessment, ‘Federal Information Technology: Electronic Record Systems and Individual Privacy, OTA – CIT – 296 (Washington, DC: U.S. Government Printing Office, June 1986).

⁵⁴¹ *Paul v Davies*, 424 U.S. 693 (1976).

The following sections will list the milestone case law that established the right to data protection in the U.S.

In *Whalen v Roe*,⁵⁴² the court considered whether a statute⁵⁴³ violated the right to information privacy for creating a centralised file of the names and addresses of patients prescribed medicines containing narcotics.⁵⁴⁴ The right to privacy enshrined in the Fourth Amendment was also considered in *Nixon v Administrators General Service*⁵⁴⁵ regarding the legitimate expectation of privacy in presidential papers. The court found that the appellant's privacy interest was overruled by that of the public interest.⁵⁴⁶

The next section will consider the Federal Trade Commission Act, which empowered the Federal Trade Commission and among other things prevents unfair methods of competition and enforces COPPA.

4.3.2. The U.S. Federal Trade Commission's information practices

The Federal Trade Commission Act of 1914⁵⁴⁷ established the Federal Trade Commission ('FTC'), which prohibits unfair and deceptive trade practices in commerce.⁵⁴⁸ A 'deceptive practice' in trade is defined as a representation that is likely to mislead the consumer.⁵⁴⁹ Section 5 of the Federal Trade Commission Act

⁵⁴² *Whalen v Roe*, 429 U.S. Reports (February 22, 1977) [589] [604].

⁵⁴³ U.S. Congress, Office of Technology Assessment, 'Federal Information Technology: Electronic Record Systems and Individual Privacy, OTA – CIT – 296 (Washington, DC: U.S. Government Printing Office, June 1986).

⁵⁴⁴ *Whalen v Roe*, 429 U.S. Reports (February 22, 1977) [591].

⁵⁴⁵ *Nixon v Administrators of General Services*, 433 U [425].

⁵⁴⁶ Gary R. Clouse, 'The Constitutional Right to Withhold Private Information' (1982) 77 *Northwestern University Law Review* 536; *McElrath v Califano*, 615 F.2d 570 (3d Cir. 1980); *St Michael's Convalescent Hospital v California*, 643 F.2d 1369 (9th Cir. 1981).

⁵⁴⁷ Federal Trade Commission Act 15 U.S.C. ss. 41–58.

⁵⁴⁸ *Ibid* Section 45(a)(1).

⁵⁴⁹ Federal Trade Commission Act section 5: unfair or deceptive acts or practices
<<https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf>> accessed 27 June 2016.

empowers the FTC to enforce COPPA⁵⁵⁰ and bring enforcement action against the companies that violate their privacy policies.⁵⁵¹

4.3.2.1. Websites to post clear and conspicuous privacy notice

In the U.S., there is generally no applicable law to regulate privacy policies online. Federal laws⁵⁵² and the FTC protect consumers and enhance competition across the economy.⁵⁵³ The FTC requires consumer-oriented commercial websites that collect personally identifying information from consumers to publish certain information⁵⁵⁴ such as posting a clear and conspicuous notice to data subjects of the type of information they will collect.⁵⁵⁵

4.3.2.2. Section 5 Federal Trade Commission Act

The FTC's primary legal authority comes from Section 5,⁵⁵⁶ which prohibits unfair or deceptive practices in the marketplace.⁵⁵⁷ The FTC can enforce terms of privacy policies and investigate and prosecute deceptive and anti-competitive business

⁵⁵⁰ 15 U.S.C. ss. 6501–6506; Federal Trade Commission 2014 Privacy and Data Security Update (2014) <https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf> accessed 27 June 2016.

⁵⁵¹ Ibid.

⁵⁵² Fair Credit Reporting Act, 15 U.S.C. s.1681.

⁵⁵³ Privacy and Data Security Update (Federal Trade Commission January 2016) <<https://www.ftc.gov/reports/privacy-data-security-update-2015>> accessed 1 March 2017.

⁵⁵⁴ 'Privacy Online: Fair Information Practices in the Electronic Marketplace' (Federal Trade Commission, May 2000) <<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>> accessed 2 February 2017.

⁵⁵⁵ How the information is collected (e.g. directly or through non-obvious means such as cookies); how they use it; how they provide choice, access and security to consumers; whether they disclose the information collected to other entities; and whether other entities are collecting information through the site. Websites will inform data subjects on how personally identifying information is used beyond the purpose for which it was collected (e.g. to conclude a transaction). The choice would encompass both internal secondary uses (such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions) and external secondary uses (such as disclosing/sharing/transferring data to third parties).

⁵⁵⁶ Federal Trade Commission Act.

⁵⁵⁷ 'Privacy and Data Security Update' (Federal Trade Commission, January 2016) <<https://www.ftc.gov/reports/privacy-data-security-update-2015>> accessed 1 March 2017; 15 USC s.45.

conduct, including unfair methods of competition.⁵⁵⁸ Recently, the FTC was successfully able to bring charges against Turn Inc., a digital advertising company in California, for deceptively enabling sellers to target digital advertisements to consumers by tracking them online and through their mobile applications. The tracking occurred even after consumers took steps to opt out of such tracking.⁵⁵⁹

In November 2010, the FTC settled charges against EchoMetrix for failing to adequately inform parents using its web monitoring software, that information collected about their children would be disclosed to third-party marketers.⁵⁶⁰

Since its inception, the FTC has successfully been able to bring enforcement action against many companies. Academic Alden Abbott is uncertain about the imposition of excessively regulatory burdens on legitimate businesses.⁵⁶¹ According to him, stringent data security practices will incur costs, which would in part be passed onto the consumer and should be weighed against the cost in reduced breaches.⁵⁶²

⁵⁵⁸ Federal Trade Commission; Promotion of Export Trade and Prevention of Unfair Methods of Competition, [15 U.S.C. ss. 41–58](#).

⁵⁵⁹ 'Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and through Their Mobile Devices' (Federal Trade Commission, 20 December 2016) <<https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively>> accessed 2 February 2017; 'Sears Settles FTC Charges Regarding Tracking Software' (Federal Trade Commission, 4 June 2009) <<https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software>> accessed 2 February 2017.

⁵⁶⁰ 'EchoMetrix Inc.' (Federal Trade Commission, 30 November 2010) <<https://webcache.googleusercontent.com/search?q=cache:6QV5M1D8u4kJ:https://www.ftc.gov/enforcement/cases-proceedings/102-3006/echometrix-inc+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2017.

⁵⁶¹ Alden Abbott, 'The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?' (The Heritage Foundation, 10 September 2014) <<https://webcache.googleusercontent.com/search?q=cache:c2vWth7rOlsJ:https://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 27 June 2016.

⁵⁶² Dissenting Statement of Orson Swindle (Federal Trade Commission) <<https://www.ftc.gov/public-statements/2000/07/dissenting-statement-commissioner-orson-swindle-ftcs-online-profiling>> accessed 28 June 2016; *FTC v LabMD* No. 1:12-cv-3005 (N.D. Ga. Nov. 26, 2012); 'Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings' (Federal Trade Commission, 12 November 2013). <<https://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf>> accessed 28 June 2016.

It is questionable whether excessive regulation will have the required desired effect. The ability of the FTC to undertake expensive investigative procedures, based on harm that has mere speculative existence, will pre-emptively coerce companies into quickly agreeing to the FTC's invasive consent decree terms.⁵⁶³ The FTC has authority to enforce COPPA,⁵⁶⁴ which protects the digital privacy rights of children under 13 years. The next section will consider the main provisions of COPPA.

4.3.3. The Children's Online Privacy Protection Act

In 1997, consumer watchdog the Centre for Media Education declared that the children-based website KidsCom.com violated Section 5.⁵⁶⁵ The FTC presented a report to Congress in 1998, discussing the lack of regulation to protect children's digital privacy.⁵⁶⁶ It advised Congress of the need for parents to understand the risks to children's digital privacy, and for the requirement of parental consent before the collection of children's personal information.⁵⁶⁷

⁵⁶³ Some businesses such as SMEs (small and medium enterprises) would find it difficult to incorporate such expensive security mechanisms. The FTC should review its policies and, while ensuring maximum data security, it should introduce cheaper means to do so. Alden Abbott, 'The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?' (The Heritage Foundation, 10 September 2014) <<https://webcache.googleusercontent.com/search?q=cache:c2vWth7rOlsJ:https://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 27 June 2016.

⁵⁶⁴ Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505.

⁵⁶⁵ Joshua Warmund, 'Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act' (2001) 1(11) *Fordham Intellectual Property Media & Entertainment Law Journal* 189, 189–215.

⁵⁶⁶ 'Privacy Online: A Report to Congress' (Federal Trade Commission, June 1998) <<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>> accessed 11 July 2016.

⁵⁶⁷ *Ibid.*

In response to this report, Congress introduced COPPA in October 1998⁵⁶⁸ to address the growing concerns around children’s digital privacy⁵⁶⁹ from online marketing and data tracking techniques.⁵⁷⁰

4.3.3.1. Meaning of ‘websites directed to children’

COPPA⁵⁷¹ affects websites that are directed to children under 13 years of age and knowingly collect information from them.⁵⁷² Since COPPA does not define ‘websites directed to children’, websites and app developers find it hard to determine whether COPPA applies to them. The FTC will consider subject matter, visual and audio content, the use of animated characters or other child-oriented activities and incentives, ads on the site or services, and other reliable evidence about the age of the actual or intended audience to determine whether the website is directed to children.⁵⁷³

The application of COPPA was extended recently when the FTC brought a complaint against a popular app targeting a general audience with an age-gate but that was still collecting information from children under 13 years of age.⁵⁷⁴ Since it only extends protection to children under 13 years, teenagers aged 13–17 remain exposed to ruthless data processing practices by commercial enterprises.

⁵⁶⁸ ‘What Is COPPA’ (TechTarget, May 2010) <<http://searchcrm.techtarget.com/definition/COPPA>> accessed 1 July 2010.

⁵⁶⁹ Susan B. Barnes, ‘A Privacy Paradox: Social Networking in the United States’ (2006) 11(9) First Monday <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312>> accessed 2 July 2016.

⁵⁷⁰ Gwenn Schurgin O’Keeffe and Kathleen Clarke-Pearson, ‘The Impact of Social Media on Children, Adolescents, and Families’ (2011) 127(4) Pediatrics 800.

⁵⁷¹ Children’s Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505.

⁵⁷² Ibid.

⁵⁷³ ‘Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business’ (Federal Trade Commission, June 2013) <<https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>> accessed 4 March 2017.

⁵⁷⁴ Joanne Furtch, ‘COPPA Is Not Just for Kid’s Websites Anymore’ (iapp, 28 October 2014) <<https://iapp.org/news/a/coppa-is-not-just-for-kids-websites-anymore/>> accessed 5 March 2017.

COPPA does mention a ‘prominent’ and ‘clearly labelled’ privacy notice. It fails to define these terms.⁵⁷⁵

4.3.3.2. Parental consent mechanism under COPPA

COPPA applies to operators of general audience websites or online services with actual knowledge of collecting information from children under 13 years.⁵⁷⁶ Neither COPPA nor FTC defines a ‘general audience website’ or the method for the operator to determine ‘actual knowledge’.

COPPA requires operators to obtain ‘verifiable parental consent’ from parents/guardians before collecting data from under 13s.⁵⁷⁷ The Act does not define ‘parental consent’ but provides certain mechanisms to achieve it.⁵⁷⁸ The FTC has provided a non-exhaustive list of parental consent mechanisms to obtain verifiable consent such as sending a notice to the email address of a parent who can verify their child’s membership.⁵⁷⁹

⁵⁷⁵ COPPA § 312.4(d).

⁵⁷⁶ ‘Complying with COPPA: Frequently Asked Questions’ (Federal Trade Commission, 20 March 2015) <<https://webcache.googleusercontent.com/search?q=cache:xn1ZBa1ByYoJ:https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2017.

⁵⁷⁷ COPPA Section 312.5(a).

⁵⁷⁸ 16 CFR Section 312.5(b).

⁵⁷⁹ Federal Trade Commission, ‘Protecting Kid’s Privacy Online Reviewing the COPPA’ (Federal Trade Commission, 2 June 2010) <<https://www.ftc.gov/news-events/events-calendar/2010/06/protecting-kids-privacy-online-reviewing-coppa-rule>> accessed 12 May 2017. It can include ‘providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using email accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph. There are additional steps such as sending a confirmatory email to the parent following receipt of consent. 16 CFR Section 312.5.

4.3.3.3. Adequacy of the parental consent mechanism

Age verification and identity authentication technologies are appealing in concept but challenging in terms of effectiveness.⁵⁸⁰ It is never certain whether the person attempting to verify identity is their actual identity or someone else's.⁵⁸¹ The FTC and corporate industry should invest in innovating methods that can ensure the identity of the parent or reduce the importance attached with consent authorising data processing.

4.3.3.4. The amended COPPA

COPPA was amended by the Federal Trade Commission on 19 December 2012, the amendment taking effect on 1 July 2013.⁵⁸² The amended rule requires website operators to disclose three categories of information: their name, address, telephone number and email address; a description of the information collected from children; and the right for parents to review or have deleted the child's personal information and refuse to permit further collection or use of the information.⁵⁸³ Parents are empowered to request a review of their children's personal information⁵⁸⁴ and refuse collection of personal information about their child.⁵⁸⁵

Section 312.7 of the amended rule prohibits the conditioning of children's participation in a game such as offering a prize that will encourage them to disclose

⁵⁸⁰ Berin Szoka and Adam Thierer, 'COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech' (2009) 16(11) *The Progress & Freedom Foundation*.

⁵⁸¹ *Ibid.*

⁵⁸² 'Complying with COPPA : Frequently Asked Questions' (Federal Trade Commission) <<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>> accessed 8 May 2017.

⁵⁸³ Children Online Privacy Protection Act 16 C.F.R. § 312.4(d).

⁵⁸⁴ 16 CFR Section 312.6 & 312.6(a)(1).

⁵⁸⁵ 16 CFR Section 312.6(a)(2).

information than is reasonably necessary to participate in the activity. The operator is also required to establish, and both maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.⁵⁸⁶

4.3.3.5. How the Federal Trade Commission enforces COPPA

The FTC has taken over 500 companies to court for non-compliance with data privacy laws.⁵⁸⁷ The FTC brought a complaint against two app developers, LAI Systems and Retro Dreamer, for allowing third-party advertisers to collect personal information (persistent identifiers)⁵⁸⁸ from children without providing notice or obtaining parents' consent.⁵⁸⁹ They will pay a combined US \$360,000 in civil penalties.

In November 2015, the FTC approved a new method of obtaining verifiable parental consent.⁵⁹⁰ The method, known as 'face match to verified photo identification' (FMVPI) and submitted by Riyo Verified Ltd., contains a two-step process. In the first step, a parent provides an image of their photo identification, which is verified as an authentic government-issued identification. In a second step, the parent is then

⁵⁸⁶ 16 CFR Section 312.8.

⁵⁸⁷ Edith Ramirez, 'Federal Trade Commission' (Federal Trade Commission, 9 January 2017) <https://www.ftc.gov/system/files/documents/public_statements/1049563/ramirez_swiss_privacy_shield_letter.pdf> accessed 1 March 2017; 'Federal Trade Commission 2013 Privacy and Data Security Update' (Federal Trade Commission) <<https://www.ftc.gov/reports/privacy-data-security-update-2013>> accessed 1 March 2017.

⁵⁸⁸ Persistent identifier is permanently attached to a digital object such as a person being assigned a unique number that identifies him/her to various parties and remains the same no matter where he/she moves to online Persistent identifiers (USGS) <<https://www2.usgs.gov/datamanagement/preserve/persistentIDs.php>> accessed 1 March 2017; 'Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act' (Federal Trade Commission, 17 December 2015) <<https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens>> accessed 1 March 2017.

⁵⁸⁹ 'Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act' (Federal Trade Commission, 17 December 2015) <<https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens>> accessed 1 March 2017.

⁵⁹⁰ 'FTC Grants Approval for New COPPA Verifiable Parental Consent Method (Federal Trade Commission, 19 November 2015) <<https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>> accessed 1 March 2017.

prompted to provide a picture taken with a phone or web camera, which is analysed to confirm that the photo is of a live person and not a still photo. The image is then compared to the identification photo using facial recognition technology to confirm whether the person submitting the photo is the one in the identification. The process includes certain privacy safeguards such as requiring encryption and prompt deletion of any personal information that is collected.⁵⁹¹

COPPA is a federal law protecting children’s digital privacy, and the FTC enforces COPPA and prevents websites based in the U.S. from operating unfair trade practices. The following sections will consider the state laws of California, Delaware and Washington to protect users’ digital privacy.

The reason for selecting the data privacy laws of these states and not others is because the U.S.-based videogames nominated for the multiple case study are governed by the laws of California, Delaware or Washington. Another reason for the choice of states is the spectrum of protection accorded within the U.S. On one side of the spectrum is California, which operates beyond the Californian borders and provides the highest levels of online protection to its citizens. Delaware has extended protection by defining anyone as a child under the age of 18 years. On the other side of the spectrum is Washington, which lacks a data privacy regime but continues to govern data handling practices of websites.

⁵⁹¹ Ibid.

4.4. California's Online Privacy Protection Act 2003

CalOPPA⁵⁹² requires websites to meet broad criteria for the presentation of privacy policies. CalOPPA will apply when a website collects 'personally identifiable information' from online users residing in California.⁵⁹³ CalOPPA has a very broad application across Californian borders because neither the data-collecting web server nor the company has to be situated in California.⁵⁹⁴ As long as the website collects information from residents in California, CalOPPA will apply.⁵⁹⁵

CalOPPA requires websites to feature a conspicuous privacy policy, which should identify the types of personal information collected and the categories of third-party entities with which the operator may share that information.⁵⁹⁶ Website operators will have to: provide a description of how consumers may review or request changes to personal information collected through the website or service;⁵⁹⁷ describe how the operator will notify consumers regarding material changes to the privacy policy;⁵⁹⁸ and list the date on which the privacy policy becomes effective.⁵⁹⁹

4.4.1. Meaning of 'conspicuously post'

The dictionary definition of 'conspicuous' is clearly visible.⁶⁰⁰ The Act defines 'conspicuously post' privacy policy as posting on the homepage of the website or first

⁵⁹² California Online Privacy Protection Act 2003 – California Business and Professions Code sections 22575–22579.

⁵⁹³ Ibid.

⁵⁹⁴ John Yates and Paul Arne, 'Protecting Your Visitors: California's Online Privacy Protection Act Could Set Standards' (LocalTechWire) <https://www.mmmlaw.com/files/documents/publications/article_228.pdf> accessed 4 March 2017.

⁵⁹⁵ Ibid.

⁵⁹⁶ CalOPPA 22575(b)(1).

⁵⁹⁷ CalOPPA 22575(b)(2).

⁵⁹⁸ CalOPPA 22575(b)(3).

⁵⁹⁹ CalOPPA 22575(b)(4).

⁶⁰⁰ Conspicuous, Oxford Dictionary <<https://en.oxforddictionaries.com/thesaurus/conspicuous>> accessed 29 March 2018.

significant page after entering the website.⁶⁰¹ This means that it should be easily visible on the homepage so that users can conveniently access the document. It also requires: an icon that contains the word 'privacy' in a colour different from the homepage's background and hyperlinks to the homepage or first significant page after entering the website;⁶⁰² a text link that hyperlinks to a webpage on which the actual privacy policy is posted⁶⁰³ and includes the word 'privacy';⁶⁰⁴ is written in capital letters equal to or greater in size than the surrounding text;⁶⁰⁵ is written in larger type or in contrasting type, font or colour to the surrounding text of the same size or is distinguishable from surrounding text on the homepage.⁶⁰⁶

4.4.2. California's Attorney General

The Office of the Attorney General protects the interests and rights of the people of California through a broad range of duties.⁶⁰⁷ The FTC complements the California attorney general,⁶⁰⁸ who continues to shape privacy and security standards in the U.S., by providing guidance and bringing law enforcement action against perpetrating organisations.⁶⁰⁹ The rules acquired by the Attorney General's Office for privacy and data security have also been adopted by companies across the U.S.⁶¹⁰

⁶⁰¹ CalOPPA 22577(b)(1).

⁶⁰² CalOPPA 22577(b)(2).

⁶⁰³ CalOPPA 22577(b)(3).

⁶⁰⁴ CalOPPA 22577(3)(A).

⁶⁰⁵ CalOPPA 22577(3)(B).

⁶⁰⁶ CalOPPA 22577(3)(C).

⁶⁰⁷ State of California Department of Justice, 'About the Office of the Attorney General' <<https://oag.ca.gov/office>> accessed 24 January 2017.

⁶⁰⁸ The California attorney general is a law enforcement official, protecting the interests of California through a broad range of duties including safeguarding public from violent criminals, helping victims of identity theft, illegal business practices, consumer crimes etc.

⁶⁰⁹ Hogan Lovells, 'California Continues to Shape Privacy and Data Security Standards' (iapp) <<https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/>> accessed 1 October 2013.

⁶¹⁰ Ibid.

The Attorney General's Office brought a lawsuit against Kaiser Permanente for unreasonably delaying the revealing of a 2011 data breach to affected individuals,⁶¹¹ state attorney generals were seen to be taking a more active role in protecting consumer data privacy online. In November 2013, 37 state attorneys general settled with Google for US \$17 million over Google's alleged violations of data privacy laws when it allowed third-party cookies on Apple's Safari browser after it told users that Safari's default settings would block such cookies.⁶¹²

The next section will consider the data privacy law of the state of Delaware.

4.5. Delaware's Online Privacy Protection Act

The state of Delaware has enacted its own specific data privacy law, which is an amalgamation of COPPA and CalOPPA. The biggest achievement of this law is to have defined a child as anyone under the age of 18 years and thus broadened the scope of protection under DOPPA.⁶¹³

On 1 January 2016, the state of Delaware enacted DOPPA. It is a combination of the privacy notice requirements in CalOPPA and compliments the online privacy rights of children in COPPA.⁶¹⁴ DOPPA defines a child as anyone under the age of 18 years⁶¹⁵ and applies to 'users' of websites,⁶¹⁶ whereas CalOPPA applies to 'consumers'.⁶¹⁷ Both terms 'users' and 'consumers' can be used interchangeably but, while a 'user' is

⁶¹¹ *The People of the State of California v Kaiser Foundation Health Plan Inc.* Case number RG14711370.

⁶¹² Claire Can Miller, 'Google to Pay \$17 Million to Settle Privacy Case' *The New York Times* (19 November 2013) <<http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?mcubz=1>> accessed 21 August 2017.

⁶¹³ Title 6 Commerce and Trade Subtitle II Other Laws Relating to Commerce and Trade Chapter 12c. Online and Personal Privacy Protection.

⁶¹⁴ 15 U.S. Code § 6501(1).

⁶¹⁵ DOPPA § 1202C(1).

⁶¹⁶ DOPPA § 1202C(4).

⁶¹⁷ CalOPPA 22575(a).

a person who can use or operate something, a 'consumer' is usually considered a person that purchases something for personal use. Hence, DOPPA can apply to people who, apart from other things, visit a website without consuming any services. A consumer on the other hand might be expected to engage with the game at a more personal level before CalOPPA applies to them. DOPPA introduces additional protection for children by placing restrictions on certain types of online marketing or advertising directed to children.⁶¹⁸

The next section will discuss Washington State's data privacy law. Washington was selected because it governs some of the videogame website privacy policies chosen for the study. It also exhibits problems because there is no law which deals with individuals' digital privacy. Instead, users are expected to consult their constitutional right to privacy, which does not make a direct reference to informational privacy.

4.6. Washington State privacy laws

Washington State's privacy laws are divided amongst several statutes that govern various aspects of privacy law. The Office of the Chief Information Officer is authorised to establish categories for data classification to create state-wide technology policy and standards.⁶¹⁹ However, this information is relevant only when there is a data breach by a public authority. There is no information on what happens if the breach is committed by a website operator or private party.

⁶¹⁸ DOPPA § 1204C. This provision is very similar to the marketing prohibitions contained in California Business & Professions Code California Business & Professions Code Section 22580; The list includes alcoholic beverages, firearms or handguns, tobacco, cigarette, dangerous fireworks, drugs paraphernalia, obscene matter etc. DOPPA 22580(i); DOPPA § 1204C(b).

⁶¹⁹ SLDS Spotlight Privacy Classifications for Washington's Data (SLDS)
<https://nces.ed.gov/programs/slds/pdf/Privacy_Classifications_for_Washingtons_Data_May2015.pdf>
accessed 5 March 2017.

The starting point is Washington State’s constitutional right to privacy. Article 1 Section 7 of the constitution states that ‘No person shall be disturbed in his private affairs, or his home invaded, without authority of law’. The law does not directly deal with privacy in the digital age.⁶²⁰

It is not clear whether CalOPPA will complement Washington State’s constitutional right to privacy owing to its broad application. Similarly, will the jurisdiction of FTC be applicable to enforce Section 5 to unfair trade practices?

4.7. Findings from the U.S.-based data privacy laws

The above study indicates there is a piecemeal approach towards data protection and privacy across the U.S. COPPA exclusively protects children’s digital privacy rights. But it only applies to children under 13 years of age, leaving children aged 13–17 to commercial exploitation. It also suffers from clarity issues such as what is meant by ‘websites directed to children’. Another purported difficulty is with obtaining a ‘verifiable parental consent’. Obtaining verifiable parental consent is questionable, especially when children can find ways around this requirement by providing false ages or fictitious email addresses. This thesis proposes that website operators should avoid relying on consent as a legitimate basis for processing. They should follow the ICO’s guidelines on employing other data protection principles based on transparency and fairness (*see footnote 113-115; 680-682*). However, as the EU and

⁶²⁰ Ibid. The rapid advances in technology meant that there were new methods of invading individuals’ private affairs. Privacy can mean many things but ‘privacy’ in the digital age would mean the collection, disclosure, and use of personal information by known and unknown government and corporate entities; Privacy Modelling Tool (watech) <https://watech-beta.herokuapp.com/user_guide> accessed 5 March 2017. If an individual has a reasonable expectation that their personally identifiable information is private, the data should remain private unless consent is obtained to collect it.

US data protection and privacy laws provide for parental consent,⁶²¹ it is recommended that a clearly presentable and easy to operate parental consent method should be placed within a privacy policy.

State-based laws such as CalOPPA and DOPPA have extended data privacy protection by building on the procedural requirements in COPPA and placed substantive limitations on internet service providers and advertisers from targeting children with harmful material such as tobacco and alcohol.⁶²² COPPA will consider 'websites directed to children' with the aid of the FTC that will recognise several factors to determine if this is so.⁶²³ DOPPA adds other potential factors such as age of models, subject matter and language along with audience composition to determine if the website is directed to children. Restriction from DOPPA also extends to the fact that although the website is not directed to children, it will apply if the website has 'actual knowledge that a child is using its internet service'.⁶²⁴

The U.S. does seem to be the leader in promulgating children's data privacy laws especially with regards to the presentation and content of privacy policies. However, there is still criticism that U.S. laws are not applied stringently. Perhaps this is because in the EU data protection has been equated with an individual's right to privacy, which is a fundamental human right that is enshrined in multiple domestic laws and international agreements. In contrast, the U.S. observes data protection as preventing 'unfair trade practices' and ensuring children's data is protected. The fact

⁶²¹ Children's Online Privacy Protection Act 16 CFR 312.5 – Parental consent; EU GDPR Article 8(1).

⁶²² DOPPA section 1204(C)(f).

⁶²³ Federal Trade Commission, 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business' <<https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>> accessed 29 March 2018.

⁶²⁴ DOPPA Section 1204(C) (b) & (c).

that the EU seriously deals with data protection can be seen from its numerous efforts to maximise individuals' right to manage and protect their data online. As discussed earlier in Chapters 1 & 2, the EU GDPR 2018 took effect on 25th May 2018 and applies uniformly across all EU member states.⁶²⁵ It overhauled the entire data privacy regime in the EU, and recognised children as a special class of data subjects. For the first time; the EU GDPR 2018 identified the possibility that children may be less risk averse online.⁶²⁶ That data processing information should be presented to them in plain and simple language.⁶²⁷ Businesses situated in the U.S. will have to meet the standards set by the EU GDPR 2018 if they want to continue doing business with EU nationals. Such robust measures are not observed in the U.S.

Although the U.S. champions the cause of children's digital privacy rights, the EU is a front runner in terms of actual safeguards concerning provisions on data privacy such as the types of personal data that need protecting (*see 3.2.1*), legitimate processing that adheres to principles of purpose limitation and proportionality (*see 3.2.3.2–3.2.3.4*), rules on consent (*see 3.2.5*), and most importantly rules on transferring personal data to third countries (*see 3.2.6*). It has started to follow the US model by introducing provisions to protect children's digital privacy (*see 3.2.4*).

The EU GDPR 2018 has empowered data subjects in controlling the processing of their data through consent. It has strengthened data privacy concepts that were earlier established in Directive 95/46/EC such as principles of minimality, digital profiling and subject access requests. It treats children as a special class of data subjects for

⁶²⁵ 'GDPR Overview: Site Portal' <<https://www.eugdpr.org/>> accessed 16 March 2018.

⁶²⁶ EU GDPR 2018 Recital 38.

⁶²⁷ EU GDPR 2018 Recital 58.

instance, profiling which is the automated processing of personal data should not concern children.⁶²⁸ This mirrors the US model establishing special rights for children.

Washington State does not provide for any data privacy laws and continues to govern website privacy policies. Users will remain in the dark about the rights and obligations they are entitled to under the parent legislation. U.S. data privacy law should incorporate robust data privacy mechanisms and maintain high standards such as that used in the EU GDPR 2018 to empower their data subjects.

Having defined the EU and the U.S. data privacy laws, the next section will consider data privacy concepts from a global perspective. Most data privacy rules are influenced by the principles established in the Fair-Trade Practices that will be considered briefly below.

4.8. Global information guidelines: Fair Trade Practices

Most democratic states apply the widely accepted fair information practices (FIPs),⁶²⁹ which set certain principles to regulate the relationship between website operator and data subject. There must be no secret personal data record-keeping systems; individuals should be able to find out the information kept about them and amend/correct and/or delete it and prevent the information from being repurposed without their consent; and the organisation holding the data must take precautions to prevent misuse of the data.⁶³⁰

⁶²⁸ EU GDPR Recital 71.

⁶²⁹ Privacy Online (Federal Trade Commission)

<<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>> accessed 6 March 2017.

⁶³⁰ Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Records, Computers and the Rights of Citizens) <<https://www.hsdl.org/?view&did=479784>> accessed 5 March 2017.

The previous sections discussed the data privacy laws representing the jurisdictions of California, Delaware and Washington. The next section will regard Canada's data privacy law, PIPEDA. Canada is one of the major contributors to the gaming industry.⁶³¹ The literature review for this thesis is based on Sara Grimes's case study relating to the privacy issues of market research strategies in children's videogames.⁶³² PIPEDA is also another front runner in data privacy law, hailed as adequate for transferring personal data from EU to Canada by Directive 95/46/EC. It did not need to comply with the Safe Harbour Principles which were levied on the U.S. at the time.⁶³³ However, the law does not address children's digital privacy rights. It is still important to consider the data privacy protections offered by Canada.

4.9. Canada's Personal Information Protection and Electronic Documents Act 2000

Canada advances data protection and privacy law on a constitutional footing,⁶³⁴ with provincial, territorial and federal privacy statutes regulating the use, collection, retention and disclosure of personal information. The Privacy Act of 1983 governs the federal institution's activities of collecting and processing personal information,

⁶³¹ Have Ontario and Quebec Eclipsed Vancouver in the Video Game Industry? <<http://studymagazine.com/2013/07/29/have-ontario-and-quebec-eclipsed-vancouver-in-the-video-game-industry/>> accessed 18 August 2017.

⁶³² Grace Chung and Sara M. Grimes, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2005) 30(4) Canadian Journal of Communication.

⁶³³ European Commission, 'Data Protection: Commission Recognises Adequacy of Canadian Regime' (Europa, 14 January 2002) <http://Europa.eu/rapid/press-release_IP-02-46_en.htm?locale=en> accessed 29 March 2018.

⁶³⁴ Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982 Section 8 (right against unreasonable search and seizure); Section 7 (right to life, liberty and security of a person) of the Charter of Rights and Freedoms.

whereas PIPEDA,⁶³⁵ passed in 2001, regulates the processing of personal information by private-sector organisations.⁶³⁶

PIPEDA governs the collection, use and disclosure of personal information by companies. It sets out a list of 10 principles which organisations 'must follow when collecting, using and disclosing personal information during commercial activity'.⁶³⁷

PIPEDA is a consent-based statute but, to date, authorities have struggled with the realities and demands of a commercial environment when operating a consent-based regime.⁶³⁸

However, PIPEDA needs to be updated with respect to children's digital privacy as well as ensure compliance with the EU GDPR 2018.

The Public Interest Advocacy Centre stated in its report that the wording of PIPEDA was vague and unclear, leaving online commercial actors free to assume implied consent.⁶³⁹ A new definition for consent was introduced in Section 6.1 of the Digital Privacy Act,⁶⁴⁰ stating that consent is only valid if there is an appreciation of the nature, purpose and consequences of the collection, use or disclosure of personal information. Website operators cannot rely on lengthy, complicated and open-ended

⁶³⁵ Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5.

⁶³⁶ Jane Bailey, 'Systematic Government Access to Private-Sector Data in Canada' (2012) 2(4) International Data Privacy Law 207, 207.

⁶³⁷ Online Privacy Law: Canada (Library of Congress 6 May 2015) <<https://www.loc.gov/law/help/online-privacy-law/2017/canada.php>> accessed 1 March 2017; Schedule 1 PIPEDA. These principles comprise accountability of the organisation collecting personal information and identifying purposes for collecting personal information; individuals will need to have knowledge and consent for the collection, use or disclosure of personal information, except where inappropriate; personal information shall be limited to purposes identified; personal information shall not be used or disclosed without the individual's consent; personal information shall be accurate, up to date and kept safe; an organization shall reveal its policies and practices relating to the management of personal information; individuals shall be given access to their information and challenge its accuracy; an individual shall be able to address a challenge concerning compliance against the organisation.

⁶³⁸ PIPEDA Review Discussion Document (Privacy Commissioner of Canada July 2006) <https://www.priv.gc.ca/media/1312/pipeda_review_060718_e.pdf> accessed 14 May 2017.

⁶³⁹ Kirsten, Konzolanka, 'Publicity and the Canadian State' (University of Toronto Press 2014).

⁶⁴⁰ Digital Privacy Act (S.C. 2015, c. 32).

privacy policies which users cannot understand and don't have the time to read. This means that the wording must inform users of the risks to online privacy and therefore the need to alter their privacy settings. This can be a very powerful tool for protecting consumer privacy.

New proposals are being considered to strengthen PIPEDA on children's digital privacy rights.⁶⁴¹ In 2010, the privacy commissioner of Canada examined the practices of online tracking, profiling and targeting through the lens of PIPEDA.⁶⁴² She found ensuring children's personal information needs careful attention.⁶⁴³ At present, there are many recommendations to give better protection to the privacy of children. Some argue for consent to be altered by placing 'an additional onus on the organisation collecting, using or disclosing information to ensure that the person providing the information "understands" that he or she is providing information and the way it may be used'.⁶⁴⁴ This shows that, at present, the parental consent mechanism is not considered sufficient to provide adequate protection to children. There is concern that parental consent may still be short of ensuring that the person giving consent is indeed the parent/guardian and not someone else.

⁶⁴¹ Ibid.

⁶⁴² Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing (Office of the Privacy Commissioner of Canada May 2011) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/report_201105/> accessed 2 March 2017.

⁶⁴³ Ibid.

⁶⁴⁴ 'Government of Canada Moves to Enhance Privacy of Individuals During Commercial Transactions' (Industry Canada, 29 September 2011) <<https://www.canada.ca/en/news/archive/2011/09/government-canada-moves-enhance-privacy-individuals-during-commercial-transactions.html>> accessed 2 March 2017.

4.10. Findings

The legislative analysis of the EU, the U.S. and Canadian data protection and privacy legislation⁶⁴⁵ has uncovered four key points, namely (1) the different ages at which children can give consent; (2) the lack of clarity around the process of consent; (3) certainty and accountability of the law; and (4) that EU data protection supervisory authorities should have greater enforcement powers.

4.10.1. Age for consent

In the EU, children were classified under the umbrella term ‘data subjects’. The earlier Directive 95/46/EC did not provide special provisions for children, lacking the age at which children can furnish online consent. This has led European member states to adopt their own interpretations, such as 14 years in Germany⁶⁴⁶ and 16 years in the UK.⁶⁴⁷ The EU GDPR 2018 includes separate provisions for children, who will now be treated as a special class of data subjects.⁶⁴⁸ But allowing member states the discretion to lower the age limit to 13 will perpetuate inconsistent application. The Data Protection Act 2018 has recently set the age for online consent at 13 years.⁶⁴⁹

The EU GDPR 2018 has set the age of consent as 16 years but allowed member states the option to reduce this age to 13 years.⁶⁵⁰ Accordingly, member states

⁶⁴⁵ Chapter 3 – The current European digital privacy legislation; Chapter 4 – Data protection and privacy framework in the U.S. and Canada.

⁶⁴⁶ Carlo Piltz, ‘The European Data Protection Law and Minors – No Legal Certainty’ (German IT Law, 2014) <<http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty/>> accessed 12 January 2017.

⁶⁴⁷ Ibid.

⁶⁴⁸ EU GDPR 2018 Article 8.

⁶⁴⁹ Data Protection Act 2018 Section 9(a).

⁶⁵⁰ EU GDPR 2018 Article 8.

may adopt their own interpretation of age for consent which could give rise to uncertainty in the applicable law.

In summary, age for consent in the EU, the U.S. and Canada are set out below:

- EU 16 years (which can be reduced to 13 years).⁶⁵¹
- U.S 13 years.⁶⁵²
- Canada It does not provide an age for consent.⁶⁵³

The differing ages for consent are also observed in the U.S. COPPA protects children under 13 years of age,⁶⁵⁴ leaving teenagers aged 13–17 vulnerable to commercial exploitation and profiling, whereas DOPPA⁶⁵⁵ defines everyone under the age of 18 as a child. In Canada, PIPEDA⁶⁵⁶ does not have separate principles for children and therefore has not installed an age-gating provision. This thesis proposes that jurisdictions should agree on the common age of 18 years to protect a child online.

The application of data privacy laws extend beyond borders as a videogame may be registered in one country with a subsidiary organisation located in a different country and a child user accessing it from yet another country. It is recommended that jurisdictions should agree on a common age for consent to facilitate uniformity and clarity of principles. The UN Convention on the Rights of a Child ('UNCRC') defines a child as anyone under the age of 18 years⁶⁵⁷ but allows signatories the option to

⁶⁵¹ EU GDPR Article 8.

⁶⁵² 16 CFR §312.2

⁶⁵³ Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5.

⁶⁵⁴ 16 CFR §312.2

⁶⁵⁵ Title 6 Commerce and Trade Subtitle II Other Laws Relating to Commerce and Trade Chapter 12c. Online and Personal Privacy Protection.

⁶⁵⁶ Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

⁶⁵⁷ UN Convention on the Rights of the Child Article 1.

choose their own ages based on cultural variations (*section 1.1*) There are liberal as well as protectionist approaches towards protecting children's rights. Children under 16 are able to give consent for medical treatment if they are judged to be capable of giving decision (Gillick competency); under the Sexual Offences Act 2003, the legal age for consenting to sex is 16 years whereas the legal age for consenting to marriage is 18 years (England and Wales) unless consent is provided by a parent/legal guardian between 16 – 17 years. (Marriages Act 1949). This thesis adds to the protectionist debate and adopts the widest range for childhood as 18 years. The EU GDPR 2018 places restrictions on profiling and automated decision-making with respect to children.⁶⁵⁸ If the recommendation above is implemented, the EU GDPR 2018 will prevent profiling of children under 18 years of age.

Children under 18 years should be subjected to limited forms of data processing; whereas website operators should obtain verifiable parental consent from children under 16 years. This is in conformity with providing maximum protection to children; following the Netherlands and Hungary data protection and privacy model where children under the age of 16 years will need to provide verifiable parental consent.⁶⁵⁹ Additionally, it also complies with the EU GDPR 2018, which allows member states the option to obtain parental consent from children under 16 years of age.⁶⁶⁰

⁶⁵⁸ EU GDPR 2018 Recital 71 and 72.

⁶⁵⁹ Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information section 6(3); Dutch Data Protection Law Article 5 (Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)

⁶⁶⁰ EU GDPR 2018 Article 8.

4.10.2. Certainty and accountability of the law

Data privacy law is not clear on the protections offered to children's digital privacy. The difficulty with COPPA is the uncertainty about its application to websites as it fails to define 'websites directed towards children'. Websites and app developers find it difficult to know if COPPA will apply to them. It provides limited protection because it applies to children under 13, leaving children aged 13–17 exposed to commercial exploitation. Another purported difficulty is the ambiguity with Washington State privacy laws. There is no provision to protect individuals' digital privacy. It seems that privacy is still regulated by traditional privacy laws contained within the constitution. There is no express provision that regulates digital privacy, so, if a videogame privacy policy is governed by the laws of Washington, children would not know which law governs the terms of the privacy policy. They will not know what rights and/or obligations they are entitled to under the law. There will be limited understanding on the consequences of consent.

It is therefore important that data privacy laws provide a clear set of rules obliging website operators to determine the laws that govern the privacy policy document as well as its contents. It was in the U.S. that rules on privacy notices were most prominently laid down. Rules from the location of the privacy notice to factors that make it distinguishable from the rest of the page were dealt by COPPA, CalOPPA and DOPPA. Such rules were not mentioned in the PIPEDA and the earlier Directive 95/46/EC.

The e-Privacy Directive provides that processing of personal data should be presented in simple and comprehensible terms⁶⁶¹ but it lacks guidance on the standard for readability.⁶⁶² The EU and Canada do not present a standard for simplicity, ease in understanding the language by children, or the exact location of the privacy notice on the main webpage.

Regarding accountability, it was observed that the Privacy Shield Framework, which protects data transferred from EU to the U.S., is vague in its practice and eligibility.⁶⁶³

The EU GDPR 2018 came into force on 25th May 2018⁶⁶⁴ but in some respects, there have been limited guidance for businesses in ensuring compliance.⁶⁶⁵ Businesses need additional guidance on opt-out, how should automated profiling be interpreted? What information needs to be told to data subjects etc.⁶⁶⁶ Additionally, it is not clear how privacy frameworks will protect children's digital privacy rights. If adequate guidance is not provided, businesses will be at risk of non-compliance, causing mistrust and confusion.

⁶⁶¹ Article 29 EU Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (Europa, 13 July 2011)

<<http://webcache.googleusercontent.com/search?q=cache:FTGjFLcJhgJ:www.pdpjournals.com/docs/88081.pdf+f&cd=1&hl=en&ct=clnk&gl=uk>> accessed 31 March 2017.

⁶⁶² e-Privacy Directive Article 5(3).

⁶⁶³ European Data Protection Supervisor 'Privacy Shield: More Robust and Sustainable Solution Needed' (Europa, 30 May 2016)

<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 14 March 2017.

⁶⁶⁴ European Commission, 'Reform of EU Data Protection Rules' (Europa) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 21 December 2017.

⁶⁶⁵ Warwick Ashford, 'Only 5% of charities are ready for GDPR, survey shows' (Computerweekly.com 27 April 2018) <

<https://webcache.googleusercontent.com/search?q=cache:ePbvWrmxVAJ:https://www.computerweekly.com/news/252440101/Only-5-of-charities-are-ready-for-GDPR-survey-shows+&cd=1&hl=en&ct=clnk&gl=uk>>

accessed 17 June 2018. There are resounding worries around principles of consent and data retention in the third sector. Eight in 10 auto businesses still in the dark over GDPR, says motor ombudsman (car dealer 23 May 2018) < <http://cardealermagazine.co.uk/publish/eight-10-auto-businesses-still-dark-gdpr-says-motor-ombudsman/151493>> accessed 17 June 2018.

⁶⁶⁶ GDPR – where guidance is needed (Data protection network) <https://www.dpnetwork.org.uk/opinion/gdpr-guidance-needed/> accessed 17 June 2018.

4.10.3. Issue of consent as a legal mechanism

In data protection, consent is a key legal matter. At the EU level, Directive 95/46/EC offered limited guidance. It mentioned the requirement of ‘unambiguous consent’⁶⁶⁷ (see 3.2.5) but remained largely silent on the consent requirements from children and adults or the age range. But it required data subjects to provide consent so that their data could be used for processing.

Videogame privacy policies require children to furnish consent. Consent should be legally binding for a contractual agreement to apply. Amongst other things, the age of the consentee has to be 18 years⁶⁶⁸ or above in most contractual agreements.⁶⁶⁹ Privacy policies require consent from children under 18 years of age. In some cases, children under 13 years are required to furnish parental consent. Once consent is furnished, the website operator will collect, process and disclose personal data belonging to the user in accordance with the terms of the privacy policy.

In the UK, there are exceptions to the age of majority rule in the form of ‘necessaries’ that includes goods and services which are appropriate to a social standard and which are required by the minor (e.g. food, clothing, lodging, education) or where the contract is for the benefit of a minor, such as an employment contract.⁶⁷⁰

⁶⁶⁷ Directive 95/46/EC Article 7a.

⁶⁶⁸ Family Law Reform Act 1969 (England and Wales).

⁶⁶⁹ Minors’ Contract Act 1987.

⁶⁷⁰ Sales of Goods Act 1979 Section 3; *Nash v Inman* [1908] 2 KB 1, CA; *Fawcett v Smethurst* (1914) 84 LJKB 473; *De Francesco v Barnum* (1890) 45 Ch D 43, where a minor aged 14 years could not furnish consent because of the unreasonable terms contained in the contract.

Some jurists have attempted to explain maturity by looking at ‘Gillick competency’.⁶⁷¹ In the UK, the age at which a child can give consent for medical treatment is 16 years.⁶⁷² Children under 16 years are not legally competent to give medical consent unless they have ‘sufficient understanding and maturity to enable them to understand fully what is proposed’.⁶⁷³ This test for maturity is referred to as ‘Gillick competency’ or ‘Fraser competency’.⁶⁷⁴ Jurists have applied the Gillick test to a child’s competence to give consent in data protection.⁶⁷⁵ It is however arguable that Gillick competency cannot apply in the context of giving online consent because unlike the medical environment where a doctor can determine a child’s maturity through face to face contact, there is no such medium in the digital world which is largely faceless and lacks an equitable arbiter in place of the doctor to determine maturity. In addition, the EU GDPR has clarified the age for consent of a child as 16 years which can be reduced to 13 years.⁶⁷⁶ This means that children 13 years and above can consent to privacy policies.

According to the Art29 WP, ‘The core legal principle is that of the best interests of the child’.⁶⁷⁷ Because younger children may lack the maturity to understand the implications of giving consent, the person giving consent must have ‘parental

⁶⁷¹ Claire A. Williams and Russell Perkins, *Consent Issues for Children: A Law unto Themselves?* (2011) 11(3) BJA 99

⁶⁷² Mental Capacity Act 2005 Section 2(5); Claire A. Williams and Russell Perkins, *Consent Issues for Children: A Law unto Themselves?* (2011) 11(3) BJA 99; Sexual Offences (Amendment) Act 2000 Section 1 provides the age for consent to sex at 16 years.

⁶⁷³ *Gillick v West Norfolk & Wisbeck Area Health Authority* [1986] AC 112 House of Lords.

⁶⁷⁴ *Ibid.*

⁶⁷⁵ Mark J. Taylor and others, *When Can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research* (2017) 1–23.

⁶⁷⁶ EU GDPR Article 8

⁶⁷⁷ Article 29 EU Data Protection Working Party, ‘Opinion 2/2009 on the Protection of Children’s Personal Data (General Guidelines and the special case of schools) <http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=2&hl=en&ct=clnk&gl=uk> accessed 14 April 2018.

responsibility', but the law relating to who does and who does not have parental responsibility is complicated and often poorly misunderstood.⁶⁷⁸

Issues can also erupt with children 16–17 and in some member states 13-17 years who may not be able to understand the implications of giving online consent. There can be problems for children under 13 years with respect to verifiable parental consent if the child is in local authority care, has absent parents or there is parental disagreement.

COPPA and the EU GDPR 2018 require parental consent to validate children's use of the website services. There is guidance on the criteria for obtaining 'verifiable parental consent' but it still poses difficulty in determining whether the person giving consent is in fact the parent/guardian. The FTC and EDPS should reduce the importance attached to the ability of consent to authorise data processing.

Apart from the validity of parental consent mechanisms, the concept of online consent is a difficult one. This is because EU GDPR 2018 requires consent to be a positive, informed and unambiguous act on the part of the online user. These requirements are difficult to fulfil if children are expected to read, understand and consent to privacy policies that are hard to locate and drafted as lengthy documents, using technical and legal jargon. In addition, if privacy policies imply consent by simply visiting the website or using its services, then consent is not a positive and informed

⁶⁷⁸ Claire A. Williams and Russell Perkins, *Consent Issues for Children: A Law unto Themselves?* [2011] 11(3) BJA 99.

action on the part of the user.⁶⁷⁹ For it to be an affirmative action, users should be furnished with an accept button or a box to tick.

The Information Commissioner's Office (ICO) published guidance on the requirements of consent under the EU GDPR 2018.⁶⁸⁰ It states that, if valid consent cannot be obtained, the principles of fair data processing should be relied upon as an alternative legal basis for processing.⁶⁸¹ Website operators should depend on the data protection principles of minimality⁶⁸² (see 3.2.3.3), transparency and purpose specification⁶⁸³ (see 3.2.3.2) to ensure safety for children's digital privacy.

4.10.4. The EU data protection authorities should have stronger enforcement powers

The FTC is authorised to enforce terms of privacy policies,⁶⁸⁴ investigate deceptive trade practices and actively bring enforcement action against companies that fail to comply with legal obligations under the data privacy laws. For instance, in November 2010 the FTC brought charges against EchoMetrix for failing to inform parents that information collected about their children would be disclosed to third-party

⁶⁷⁹ Six out of ten privacy policies studied were updated in late 2017 and 2018. The rest are still implying consent even after the EU GDPR 2018 came into force. <<http://supercell.com/en/privacy-policy/>> accessed 16 May 2018. The privacy policy of Clash of Clans was updated on 25th May 2018; <<https://www.miniclip.com/games/page/en/privacy-policy/>> accessed 16 May 2018. The privacy policy of Miniclip was updated on 14 September 2017; <<https://privacy.microsoft.com/en-us/privacystatement>> accessed 16 May 2018. Minecraft privacy statement was updated in April 2018; <<https://euw.leagueoflegends.com/en/legal/privacy>> accessed 16 May 2018. League of Legends privacy policy was updated on 16 May 2018; <https://store.steampowered.com/privacy_agreement/> accessed 16 May 2018. The privacy policy of Dota 2 was revised on 23 January 2018; <<https://king.com/privacyPolicy>> accessed 16 May 2018. The privacy policy of Candy Crush Saga was updated on 24 April 2018.

⁶⁸⁰ 'ICO GDPR Guidance' (ICO, 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017.

⁶⁸¹ Ibid.

⁶⁸² Directive 95/46/EC Article 6(1)(c): The principle of minimality limits data collection to achieve the purpose behind the collection.

⁶⁸³ Directive 95/46/EC Article 6(1)(b): Under the principle of 'purpose specification', data should be gathered for a specified, legitimate and compatible purpose.

⁶⁸⁴ 'Privacy and Data Security Update' (Federal Trade Commission, January 2016) <<https://www.ftc.gov/reports/privacy-data-security-update-2015>> accessed 1 March 2017.

marketers.⁶⁸⁵ The Office of the Attorney General protects the interests and rights of the people of California through a broad range of duties.⁶⁸⁶ The FTC complements the California attorney general,⁶⁸⁷ who continues to shape U.S.-based modern-day data privacy law. The attorney general provides guidance and brings legal enforcement action against organisations failing to comply with data privacy law.⁶⁸⁸ The rules introduced by the Attorney General's Office for privacy and data security have also been adopted by companies across the U.S.⁶⁸⁹

On the European front, the Art29 WP and the EDPS are independent organisations that have advisory status. They oversee the application of data privacy law and report back to the European Commission on compliance issues. They provide guidance on data privacy law and the means for website operators to ensure compliance. The Information Commissioner's Office (ICO) is an independent regulatory authority that acts as the United Kingdom's national data protection authority. Amongst other duties, the Information Commissioner oversees the application of the Data Protection Act 1998, and now the Data Protection Act 2018 in the UK.

The Commissioner has enforcement powers to issue notices and stop orders, issue monetary penalties, prosecute those who commit a criminal offence and report to

⁶⁸⁵ 'EchoMetrix Inc.' (Federal Trade Commission, 30 November 2010) <<https://webcache.googleusercontent.com/search?q=cache:6QV5M1D8u4kJ:https://www.ftc.gov/enforcement/cases-proceedings/102-3006/echometrix-inc+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2017.

⁶⁸⁶ State of California Department of Justice, 'About the Office of the Attorney General' <<https://oag.ca.gov/office>> accessed 24 January 2017.

⁶⁸⁷ The California attorney general is a law enforcement official, protecting the interests of California through a broad range of duties including safeguarding public from violent criminals and helping victims of identity theft, illegal business practices, consumer crimes etc. State of California Department of Justice, 'About the Office of the Attorney General' (oag.ca.gov) <<https://oag.ca.gov/office>> accessed 21 December 2017.

⁶⁸⁸ Hogan Lovells, 'California Continues to Shape Privacy and Data Security Standards' (iapp) <<https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/>> accessed 1 October 2013.

⁶⁸⁹ Ibid.

Parliament.⁶⁹⁰ According to Dr Karen Mc Cullagh, an academic at the University of East Anglia, little research exists to evaluate the effectiveness of the ICO as a regulator.⁶⁹¹ She analysed that the investigative and enforcement powers of the ICO are ‘lamentably weak and ineffective’ because it lacked adequate funding and properly trained staff.⁶⁹² According to Dr Mc Cullagh, when the EU GDPR 2018 is implemented the ICO will face a budgetary deficit of £42.8m, which will add to its structural and operational weakness.

The EU should have similar data privacy authorities as in the US. Rather than having advisory status, the departments should be able to bring enforcement action against the perpetrator organisations. Similarly, national data protection authorities should be adequately funded and staffed to carry out their functions efficiently. The EU GDPR 2018 will place enormous pressures on organisations to ensure protection to data subjects. If the supervisory authorities lack teeth, it will directly impact the effectiveness of the EU GDPR 2018.

4.11. The big picture: conclusions

On a global level, current laws lack the clarity and uniformity to treat children as a special class of data subjects. This includes the age at which children can provide online consent, which differs between jurisdictions. This thesis recommends that jurisdictions should universally agree upon defining a child as anyone under the age of 18. This recommendation is in line with international obligations under the UN

⁶⁹⁰ ‘Taking Action – Data Protection’ (ICO) <<https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>> accessed 24 January 2018.

⁶⁹¹ ‘UK Data Protection Regulator Is “Ineffective,” Says Research’ (UEA) <http://www.uea.ac.uk/about/media-room/press-release-archive/-/asset_publisher/a2jEGMiFHPhv/content/uk-s-data-protection-regulator-is-ineffective-says-research> accessed 24 January 2018.

⁶⁹² Ibid.

CRC⁶⁹³ to which most countries are signatories.⁶⁹⁴ Additionally, it would be unreasonable for 18-year-olds to ask their parents for consent. Therefore, it is recommended that verifiable parental consent should be obtained from children under 16 years, which is compatible with the requirement of EU GDPR 2018.⁶⁹⁵

Another purported difficulty is with the issue of consent. It is difficult to prove, and the EU GDPR 2018 is a public legal framework that will override the private legal contracts which users are expected to consent to. Consent can be provided as per the requirement of a privacy policy, but the age range for consent differs in jurisdictions. Parents can furnish consent for children under 13 years but there is difficulty in proving the identity of the parent/legal guardian. Further, it relies enormously on the supervisory role of parents/guardians, which may not necessarily be the case.

The use of implied consent to authorise data processing abrogates the legal requirement for consent to be 'any freely given specific and informed action by the user'.⁶⁹⁶ Alternative means for processing data adhering to principles of minimality and purpose specification should be applied. Data protection authorities should be empowered to bring enforcement action against perpetrating organisations and the laws need to be clearer and precise in providing digital protection.

⁶⁹³ UN Convention on the Rights of the Child Article 1.

⁶⁹⁴ United Nations treaty collection

<https://webcache.googleusercontent.com/search?q=cache:nr6kif9nff4J:https://treaties.un.org/Pages/ViewDetails.aspx%3Fsrc%3DIND%26mtdsg_no%3DIV-11%26chapter%3D4%26lang%3Den+&cd=1&hl=en&ct=clnk&gl=uk> accessed 14 April 2018; Chapter 1 Section 1.2.3.

⁶⁹⁵ EU GDPR 2018 Article 8(1).

⁶⁹⁶ Directive 95/46/EC Article 2(h). Consent is further categorised into explicit consent which is given for sensitive data Directive 95/46/EC Article 8(2)(a). Consent is needed to ensure legitimacy of processing as well as transfer of data to third countries that do not possess adequate levels of protection. Directive 95/46/EC Article 26(1)(a).

Overall, there is a gap in children's digital privacy rights. The U.S. is the leader in promulgating laws that exclusively protect children's digital rights and rules that regulate the accessibility, prominence and content of privacy policies. On the flip side, the EU leads by providing detailed definitions on all aspects of digital privacy. But, unlike the FTC or the California attorney general in the U.S., the EU's EDPS and the Art29 WP lack the ability to bring enforcement action against offending organisations. Canada has gone a step further by codifying digital privacy as a constitutionally fundamental right but falls short of recognising the special protection needed for children's digital privacy.

The legal findings of *Chapters 3 and 4*, namely the issues of readability, principles of processing personal data, concept of consent and the use of cookies, will be applied to the multiple case study in *Chapter 5*. There will be a detailed two-part multiple case study of the privacy policies of 10 videogame websites selected for this thesis. The privacy policies of the videogames will be studied based on 11 evaluation criteria. The first part of the multiple case study (*Chapter 5*) will analyse whether privacy policies comply with expectations for children to read, understand and consent to their terms. The second part of the multiple case study (*Chapter 6*) will evaluate whether the privacy policies remain compatible with governing data privacy law.

CHAPTER 5

PART 1 – ONLINE GAMES CASE STUDIES: PRIVACY POLICIES AND CHILDREN

5.1. Introduction

Chapters 3 and 4 carried out doctrinal legal research regarding the data protection and privacy laws of the EU, the U.S. and Canada. The research facilitated functional analysis of the law by uncovering essential functions of data privacy law that should be adhered to in privacy policies. *Chapter 5* carries out the first part of the multiple case study of privacy policies of 10 videogames. The content of the privacy policies will be analysed and determine whether they comply with expectations for children to read, comprehend and consent to such terms.

Websites collect information from users of their services, in accordance with the legal requirements of their country's registration. Each videogame website should inform visitors of their intention to do so. The privacy policy details the website's data handling practices, determining what type of information is collected, what happens to the information that is collected, whether the information is shared with third parties, and what, if any, rights exist for website users to access, correct and/or delete personal information held by the website.⁶⁹⁷

A comprehensive privacy policy can help websites achieve greater legal significance and establish a relationship of trust with its customers.⁶⁹⁸ A videogame will attract a large younger audience that will be expected to read, comprehend and consent to

⁶⁹⁷ Ian J. Turnbull, *Privacy in the Workplace* (CCH Canadian Limited 2009).

⁶⁹⁸ Tom Pareigat, 'Maintaining Customer Confidence Online' (ABA Bank Compliance March/April 2001) <<https://congressional.proquest.com/central>> accessed 10 January 2017.

the policy before they can utilise its services. For a younger game player, privacy policies should present an understandable, user-friendly and unambiguous clarification of its data handling practices. For the purposes of this project, a child is anyone under the age of 18 (see 1.2.3; 4.10.1).

Sections 5.2–5.3 explains that a multiple case study is the most appropriate method for investigating privacy policies; Section 5.4 presents the criteria for evaluating privacy policies; Section 5.5 carries out the multiple case study; Section 5.6 presents comparative findings of the content analysis; Section 5.7 evaluates websites' registration procedures; and Section 5.8 presents concluding remarks and recommendations.

5.2. Children's digital privacy

Children are spending longer hours in front of a screen.⁶⁹⁹ Playing videogames is the second most popular activity carried out by children between the ages of nine and 16.⁷⁰⁰ Videogames encourage children to register and provide their personal information. Children's digital privacy is problematic because children may not be aware of digital privacy risks including profiling, commercial exploitation and misuse of personal data, identity theft, loss of reputation and discrimination.⁷⁰¹

Data privacy laws should ensure that children's digital privacy is protected when they play videogames. They should be aware of the data handling practices of websites.

⁶⁹⁹ Kim Bartel Sheehan, *Controversies in Contemporary Advertising* (SAGE 2014).

⁷⁰⁰ Sonia Livingstone and others, 'Risks and Safety for Children on the Internet: The UK Report' (The London School of Economics and Political Science, December 2010).

<[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/National%20Reports/UKReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20Reports/UKReport.pdf)> accessed 17 November 2017.

⁷⁰¹ Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) *Information & Communications Technology Law* 146.

Privacy notices should be accessible, concise and easy to understand. Chapters 3 and 4 demonstrate that the age for consent varies in different jurisdictions, provisions on parental consent mechanisms are unclear, and the law lacks provisions regulating the data handling practices of websites that are directed towards children.

The next section will consider the case study methodology for analysing the privacy policies of videogames.

5.3. Multiple case study methodology

One of the approaches for content analysis of an online videogame website is a case study methodology.⁷⁰² In the past, case study methods have been used in various disciplines such as sociology,⁷⁰³ law⁷⁰⁴ and medicine.⁷⁰⁵ A multiple case study helps in understanding the differences and similarities between cases and analyses data both within each case and across cases.⁷⁰⁶ It facilitates the exploration of wider research questions and creating a more convincing theory because the suggestions are grounded in several empirical evidences.⁷⁰⁷ Therefore, a multiple case study of 10 most popular videogame websites will produce generalised solutions that can then

⁷⁰² Robert K. Yin, *Case Study Research Design and Methods* (2nd edn, SAGE Publications 1984). Robert K. Yin defines this method 'as an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used'.

⁷⁰³ E. Grassel and B. Schirmer, 'A Prospective Longitudinal Study Investigating Expectations towards and Experience with Training and Professional Support' (2006) 39(3) *Zeitschrift Fur Gerontologie Und Geriatrie* 217.

⁷⁰⁴ George I. Lovell, 'Justice Excused: The Deployment of Law in Everyday Political Encounters' (2006) 40(2) *Law & Society Review* 283; S. Taylor and V. Berridge, 'Medicinal Plants and Malaria: An Historical Case Study of Research at the London School of Hygiene and Tropical Medicine in the Twentieth Century' (2006) 100(8) *Transactions of the Royal Society of Tropical Medicine and Hygiene* 707. It ascertains the adequacy of government programmes, such as evaluating the smoke-free law.

⁷⁰⁵ S. Taylor and V. Berridge, 'Medicinal Plants and Malaria: An Historical Case Study of Research at the London School of Hygiene and Tropical Medicine in the Twentieth Century' (2006) 100(8) *Transactions of the Royal Society of Tropical Medicine and Hygiene* 707.

⁷⁰⁶ Johanna Gustafsson, 'Single Case Studies vs. Multiple Case Studies: A Comparative Study' (2017) <<http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf>> accessed 1 May 2018.

⁷⁰⁷ Kathleen M. Eisenhardt and Melissa E. Graebner, 'Theory Building from Cases: Opportunities and Challenges' (2007) 50(1) *Academy of Management Journal*.

be applied to inform both the comparative study as well as draft the child-friendly model privacy policy in *Chapter 7*. The empirical study investigates the data handling approach of videogames towards children by applying 11 evaluation criteria to the privacy policy of each videogame. As this is an exploratory case study, discovering issues related to privacy policies, governing data privacy law and children's digital privacy rights, 10 most popular videogame websites would be sufficient for the study.⁷⁰⁸

The multiple case study design is divided into two parts. The first part will examine whether the videogame privacy policies are compatible with the expectation that children should read, understand and consent to the terms.⁷⁰⁹ The second part of the multiple case study will analyse if the privacy policies comply with governing data privacy laws.⁷¹⁰ The findings of the two-part multiple case study will provide an enriched understanding of how popular videogames handle children's personal data and moreover, whether their privacy policies comply with governing data privacy laws. It will also propose recommendations that will make the process of reading, understanding and consenting to privacy policies more child-friendly.

An exploratory comparative multiple case study design will be used to incorporate 10 videogame websites based on popularity rankings and representing the territories of the EU, the U.S. and Canada (*see 1.6.4.1*).

⁷⁰⁸ Grace Chung and Sara M. Grimes, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2005) 30(4) *Canadian Journal of Communication*. The research carried out a comparative multiple case study of 17 popular children's gaming websites to explore the prominence of market research and data mining technologies used in children's websites.

⁷⁰⁹ Chapter 5 Part 1: Online Games Case Studies: Privacy Policies and Children.

⁷¹⁰ Chapter 6 Part 2: Online Games Case Studies: Privacy Policies and Governing Data Privacy Law.

5.3.1. The study of privacy policies

The privacy policies will be studied using 11 criteria, which largely follow the order of the rules regulating data handling practices in data protection and privacy laws. The privacy policies evaluated were updated in January 2017⁷¹¹ (see 5.5.2.1).

The next section will further elaborate on the study of privacy policies by providing reasons behind choosing the legislation in the EU, the U.S. and Canada for conducting the study.

5.3.1.1. The significance of the EU, the U.S. and Canada in the gaming industry

With five European countries⁷¹² featuring in the top 10 countries ranked on global revenue estimates for 2016, the European gaming industry has become a central hub for videogames.⁷¹³ The European Commission published the ‘Support for the Development of European Video Games’ programme to inject funds into the videogame production companies for developing works with high creative value and wide cross-border exploitation potential.⁷¹⁴ With such international collaborative efforts, the EU’s gaming industry continues to boom, a fact conceded by companies

⁷¹¹ No obvious reasons were found for the update in the privacy policies. A more recent update occurred in 6 videogame websites in late 2017 and 2018.

⁷¹² Germany, the United Kingdom, France, Spain and Italy.

⁷¹³ ‘Top 100 Countries by Game Revenues’ (newzoo) <<https://newzoo.com/insights/rankings/top-100-countries-by-game-revenues/>> accessed 11 March 2017.

⁷¹⁴ Creative Europe, ‘Video Game Development’ (European Commission) <https://ec.europa.eu/programmes/creative-europe/media/video-game-development_en> accessed 6 February 2017.

as Facebook.⁷¹⁵ The U.S. and especially California have become a Mecca for the American videogames industry,⁷¹⁶ taking first place in the world.

According to the comScore report, Canadians internet usage is nearly double the worldwide average.⁷¹⁷ The significance of these three regimes in the design and development of videogames is reflected in this project's choice of comparative law analysis. However, an unintended effect is the potential data privacy breaches.

The next section will examine the rationale for selecting the 10 videogames for the multiple case study exploration.

5.3.1.2. Method of selecting the videogame websites

The cases were selected based on surveys and data statistics carried out by media audience research firms such as Statista⁷¹⁸ to retrieve the most popular videogames.⁷¹⁹ This arrangement produced a total of 20 games (including *World of Warcraft*, *Minecraft* and *League of Legends*). Most of the games were 18-rated; some of the games shared the same publisher (they shared the same umbrella privacy

⁷¹⁵ Chris O'Brien, 'Facebook Highlights the Rising Power of Europe's Gaming Industry' (VB, 11 June 2015) <<http://venturebeat.com/2015/06/11/facebook-highlights-the-rising-power-of-europes-game-industry/>> accessed 6 February 2017.

⁷¹⁶ John Gaudiosi, 'The 10 Most Successful States for Video Game Development' (*Fortune*, 24 February 2015) <<http://fortune.com/2015/02/24/10-successful-states-video-game-development/>> accessed 22 January 2017.

⁷¹⁷ Omar El Akkad, 'Canadian's Internet Usage Nearly Double the Worldwide Average' *The Globe and the Mail* (8 March 2011) <<http://www.theglobeandmail.com/technology/tech-news/canadians-internet-usage-nearly-double-the-worldwide-average/article569916/>> accessed 2 January 2017; Christian Nutt, 'Canada's Game Dev Industry Grows: 472 Studios, 20,400 People' (Gamasutra, 16 November 2015)

<http://www.gamasutra.com/view/news/259511/Canadas_game_dev_industry_grows_472_studios_20400_people.php> accessed 23 January 2017; Nordicity, 'Canada's Video Game Industry in 2015' (Nordicity, August 2015) <<http://www.nordicity.com/media/20151210faaebhea.pdf>> accessed 23 January 2017; The Canadian videogame industry has become the third largest in the world after the U.S and Japan, with 472 companies located throughout the country and an economic impact on Canada's GDP of \$3 billion in 2015.

⁷¹⁸ Statista is a leading statistics company that researches quantitative data, statistics and related information for large corporations and academic institutions. 'About Statista Inc.' (Statista) <<https://www.statista.com/aboutus/>> accessed 21 February 2017.

⁷¹⁹ 'Most Played PC Games on Gaming Platform Raptr in November 2015, by Share of Playing Time' (Statista, 2015) <<https://www.statista.com/statistics/251222/most-played-pc-games/>> accessed 22 January 2017.

policy); and most of the games were registered in the U.S. This meant that only four games were selected for the analysis. The aim was to select games that represent the legal jurisdictions of the U.S., Canada and the EU. The remaining games were selected by observing reviews of the most popular free videogames available on PC and mobile.⁷²⁰

5.3.1.3. Issue with selecting a Canadian videogame website

The process of selecting Canadian games proved more cumbersome. Canadian companies that developed and published popular games over time became subsidiaries of foreign companies that acquired publishing rights to those games. This includes Beenox, which developed the world-renowned game *Skylanders*⁷²¹ and then became a subsidiary of American videogame publisher Activision.⁷²² Similarly, BioWare, based in Edmonton, Canada, has developed successful franchises such as *Star Wars: The Old Republic*⁷²³ and was later bought by American videogame publisher Electronic Arts.⁷²⁴

The first Canadian game selected was *Prince of Persia*, which was developed by Ubisoft Montreal, a Canadian subsidiary of the French videogame developer Ubisoft, located in Montreal, Quebec, Canada.⁷²⁵ Since a subsidiary has a separate and distinct

⁷²⁰ Free online games: top gaming resource (TechGlamour) <<http://techglamour.com/online-free-games-gaming-resources/#sthash.LD8L65I0.dpuf>> accessed 23 January 2017.

⁷²¹ Craig Chapple, 'Licence to Thrill: Behind the Scenes at Beenox' (Develop, 23 November 2015) <<https://webcache.googleusercontent.com/search?q=cache:cKGuVtsrh9MJ:https://www.mcvuk.com/development/licence-to-thrill-behind-the-scenes-at-beenox+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 23 January 2017.

⁷²² Peter Cohen, 'Activision Buys Game Conversion Developer Beenox' (Macworld, 25 May 2005) <<https://www.macworld.com/article/1044978/beenox.html>> accessed 23 January 2017.

⁷²³ Emily Gera, 'Star Wars: The Old Republic Continues to Stay Afloat with over 1M Monthly Players' (Polygon Vox Media, 14 August 2014) <<http://www.polygon.com/2014/8/14/6001503/star-wars-the-old-republic-2014-players-ea-bioware>> accessed 23 January 2017.

⁷²⁴ Caroline McCarthy, 'Electronic Arts Pays \$860 Million for BioWare, Pandemic Studios' (cnet, 1 October 2007) <<https://www.cnet.com/news/electronic-arts-pays-860-million-for-bioware-pandemic-studios/>> accessed 23 January 2017.

⁷²⁵ Ubisoft Montreal <<http://montreal.ubisoft.com/en/>> accessed 23 January 2017.

legal entity for purposes of taxation, regulation and liability, *Prince of Persia* mildly strokes the requirement for a videogame governed by Canadian laws.⁷²⁶ But the terms of service stated that *Prince of Persia* was governed by the laws of England and not Canada.

The second Canadian game, *Princess Isabella: A Witch's Curse*, was selected in November 2015. This was created by Gogii Games, an independent developer based in Canada, and governed by Canadian laws. Recently, it was observed that the game was published by Big Fish Games Inc., which is situated in Washington State and governed by its laws.⁷²⁷

In conclusion, these two games were found to be unsuitable as their governing data privacy law is not Canadian but rather U.S. and English.

5.3.1.4. Videogame websites selected based on rankings

Table 3 ranks the games and the sources of statistical software programmes. Surveys and data statistics were consulted to find the games based on usage (i.e. percentage share of total time played, global traffic rank and revenue) in 2015 (*Chapter 5 Table 3*). Statista⁷²⁸ compiled the most played PC games worldwide in November 2015 based on the number of hours played.⁷²⁹ Most of these games were either 18+ and were not registered or governed by the laws of EU or Canada. eBizMBA⁷³⁰ helped

⁷²⁶ Mindy Bonomelli, 'Wholly-Owned Subsidiaries: Same Same but Different' (Lexology, 8 April 2014 <<https://www.lexology.com/library/detail.aspx?g=90cc6c72-de1a-4ba7-91d0-7cd7a798c5ed>> accessed 23 January 2017.

⁷²⁷ Big Fish Terms of Use <<http://www.bigfishgames.com/company/terms.html>> accessed 20 March 2017.

⁷²⁸ Statista is a leading statistics company that researches quantitative data, statistics and related information for large corporations and academic institutions. 'About Statista Inc.' (Statista) <<https://www.statista.com/aboutus/>> accessed 21 February 2017.

⁷²⁹ About Statista Inc. (Statista) <<https://www.statista.com/aboutus/>> accessed 11 March 2017.

⁷³⁰ eBizMBA is a website which ranks websites on a regular basis, and ranked the 15 most popular game sites 'The eBusiness Guide' (eBizMBA) <www.ebizmba.com/> accessed 11 March 2017.

capture a few more games. App Annie⁷³¹ was also consulted, which highlighted the top performing apps in the year 2015.⁷³² Eventually, the *Toronto Sun*⁷³³ was consulted. This is an English-language newspaper published in Toronto, Ontario, Canada,⁷³⁴ and it was consulted because it highlighted the top performing games in Canada⁷³⁵ for inclusion in the multiple case study.

All 10 games were selected based on usage popularity, with age verifications 13+ or even younger. Nonetheless, they are popular amongst all ages and a proportionate representation of the data privacy regimes of the U.S., the EU and Canada.

Key information about each of the 10 games selected for the study are set out below in Table 3 in which games were selected based on certain criteria including percentage share of total time played or global traffic or revenue.

Table 3 Online game website ranking/percentage and source (2015)

Online game website	Percentage % share of total time played	Source
<i>League of Legends</i>	22.92%	Statista < https://www.statista.com/statistics/251222/most-played-pc-games/ >
<i>Dota 2</i>	5.09%	Statista < https://www.statista.com/statistics/251222/most-played-pc-games/ >
<i>Minecraft</i>	1.97%	Statista < https://www.statista.com/statistics/251222/most-played-pc-games/ >
<i>Heroes of the Storm</i>	1.16%	Statista < https://www.statista.com/statistics/251222/most-played-pc-games/ >
Online game website	Global Traffic Rank	Source

⁷³¹ App Annie was also a business intelligence company that monitors and market reports for apps. 'The App Analytics and App Data Industry Standard' (App Annie) <<https://www.appannie.com/>> accessed 21 February 2017.

⁷³² 'The App Analytics and App Data Industry Standard' (App Annie) <<https://www.appannie.com/>> accessed 11 March 2017.

⁷³³ <<http://torontosun.com/>> accessed 21 February 2017.

⁷³⁴ Julia Alexander, '10 Best Canadian-Made Video Games' *Toronto Sun* (21 August 2013) <<http://torontosun.com/2013/08/21/10-best-canadian-made-video-games/wcm/0b267bf8-fe60-4639-8b19-8c8c6e600c54>> accessed 21 February 2017.

⁷³⁵ Ibid.

Pogo	3	eBizMBA < http://www.ebizmba.com/articles/game-websites >
Miniclip	4	eBizMBA < http://www.ebizmba.com/articles/game-websites >
Big Fish Games/Gogii Games (<i>Princess Isabella</i>)	5	eBizMBA < http://www.ebizmba.com/articles/game-websites >
Online game website	App Revenue	Source
<i>Candy Crush Saga</i>	1	App Annie < https://www.appannie.com/insights/worldwide-app-annie-index-games-may-2015/ >
<i>Clash of Clans</i>	5	App Annie < https://www.appannie.com/insights/worldwide-app-annie-index-games-may-2015/ >
Online game website	Ranking	Source
<i>Prince of Persia</i>	Not Applicable	<i>Toronto Sun</i> < http://torontosun.com/2013/08/21/10-best-canadian-made-video-games/wcm/0b267bf8-fe60-4639-8b19-8c8c6e600c54 >

5.4. Criteria for evaluating the privacy policies of videogame case studies

Videogames registered and governed by U.S. data privacy law will be evaluated using the Children’s Online Privacy Protection Act (‘COPPA’),⁷³⁶ the California Online Privacy Protection Act (‘CalOPPA’),⁷³⁷ the Delaware Online Privacy Protection Act (‘DOPPA’),⁷³⁸ Washington State’s data privacy laws and the Federal Trade Commission’s (‘FTC’) privacy policy requirements.⁷³⁹ European videogames will be evaluated against the Data Protection Directive (‘Directive 95/46/EC’),⁷⁴⁰ the ‘EU GDPR 2018’⁷⁴¹ and any guidelines provided by the Article 29 EU Data Protection

⁷³⁶ Children’s Online Privacy Protection Act of 1998 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2681-728, enacted October 21, 1998).

⁷³⁷ California Online Privacy Protection Act 2003 (California Business & Professions Code sections 22575–22579).

⁷³⁸ Delaware Online Privacy Protection Act TITLE 6 Commerce and Trade subtitle II Other Laws Relating to Commerce and Trade Chapter 12C. Online and Personal Privacy Protection.

⁷³⁹ The Annenberg Public Policy centre of the University of Pennsylvania, ‘Privacy Policies on Children’s Websites: Do They Play by the Rules?’ (Report no. 33).

⁷⁴⁰ Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁷⁴¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (Text with EEA relevance).

Working Party ('Art29 WP'), which is an advisory body for the implementation of European laws.⁷⁴²

The selection and order of the criteria for analysing privacy policies emulate the arrangement of the contents of data privacy laws. Table 4 lists the 11 criteria that will be used to evaluate the privacy policies of the multiple games study research. They are in this order because they imitate the sequence of data privacy laws regulating privacy policies.

Table 4 – List of criteria for studying privacy policies

Criteria	Questions to consider
Criterion 1 – Location of privacy policy	Is the policy located on the main webpage with a distinguishing feature such as different font, colour, size or more obscurely located, making it hard for easy visibility?
Criterion 2 – Length and wording of the privacy policy	Is the length compatible with expectations from children and their parents to read the entire document? Is it worded in easy-to-understand, standard English or does it use complicated legal and technical terms?
Criterion 3 – Governing legislation	Is there uniformity in the use of privacy protection mechanisms such as the specific governing law on data protection and privacy? Does the policy explain these rules?
Criterion 4 – Privacy rules involving the Privacy Shield Framework to safeguard transfer of data between the EU and the U.S.	Does the website define and explain the purpose behind the use of Privacy Shield Framework? Has it been defined in a child-friendly manner?
Criterion 5 – TRUSTe privacy certification	Does the website use TRUSTe safety mechanism? Does it explain what it means? Who ensures compliance with the Privacy Shield?
Criterion 6 – Collection of information from children	How much information is being collected from children? Does the policy mention and explain the type of information that is being collected and the purpose behind the collection?
Criterion 7 – Third parties collecting personal information	Do websites allow third parties to collect personal information?
Criterion 8 – Cookies and other tracking technologies	Do websites use cookies and other third-party tracking technologies? Does the policy adequately define such tracking mechanisms?
Criterion 9 – Methods to disable cookies and other third-party tracking technologies	Is there a process to disable tracking technologies? Is it sufficiently explained and easily operable by children and their parents?
Criterion 10 – Parental consent mechanism	Does the policy mention the type of parental consent mechanism that applies to the videogame?
Criterion 11 – Players' right to subject access requests	Are data subjects accorded the right to access, correct and/or delete their personal information held by the website?

⁷⁴² 'Opinions and Recommendations' (Europa)

<http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=1&hl=en&ct=clnk&gl=uk> accessed 20 March 2017.

Table 5 introduces the 10 videogames for the multiple case study, with additional details including the name, proprietor, address of the registered headquarters and the governing data privacy law. The table has been colour-coded to highlight the set of games belonging to a legislature. Pale green represents games governed by U.S. law; pale purple represents European law; a pale blue represents both U.S. and European law; and a pale orange Canadian law.

Table 5 Videogames selected for the multiple case study; their publishers and location of headquarters

- Games that are governed by U.S. law
- Games that are governed by European law
- Games that are governed by U.S. and European law
- Games that are governed by Canadian law

Videogame website	Publisher/Owner	Headquarter location	Governing data privacy law
<i>Dota 2</i>	Valve Corporation < http://www.valvesoftware.com > Age restriction 10+ ⁷⁴³ <i>Dota 2</i> is a multiplayer online battle arena (MOBA) videogame in which two teams try to destroy a structure defended by the opposing team. ⁷⁴⁴	Bellevue, Washington, United States	'...laws of the State of Washington, U.S.A.' Terms of Use (Valve Corporation)
<i>Princess Isabella</i>	Big Fish Games < www.bigfishgames.com > Age restriction 7+ ⁷⁴⁵ A hidden object game to solve puzzles, battle against magical creatures to rescue the princess's family. ⁷⁴⁶	Seattle, Washington, United States	'laws of the State of Washington, U.S.A.,' Terms of Service (Big Fish Games)
<i>Miniclip</i>	Miniclip Inc. < http://www.miniclip.com > Age restriction 11+ ⁷⁴⁷ A free-to-play online games website with a collection of games. ⁷⁴⁸	Neuchâtel, Switzerland	'The laws of England and Wales...' Terms & Conditions (Miniclip)

⁷⁴³ <<http://pixelkin.org/games/dota-2/>> accessed 1 January 2017.

⁷⁴⁴ <<http://store.steampowered.com/app/570/>> accessed 1 January 2017.

⁷⁴⁵ <<http://www.everybodyplays.co.uk/review/Princess-Isabella-A-Witches-Curse-Review/343>> accessed 1 January 2017.

⁷⁴⁶ <<http://www.iwin.com/games/princess-isabella--a-witches-curse>> accessed 1 January 2017.

⁷⁴⁷ <<https://www.common sense media.org/website-reviews/miniclip>> accessed 2 January 2017.

⁷⁴⁸ <<http://www.miniclip.com/games/en/>> accessed 2 January 2017.

<i>Prince of Persia</i>	Ubisoft < https://www.ubisoft.com/en-GB > Age restriction 13+ ⁷⁴⁹ Ubisoft Montreal – Developer & Subsidiary < montreal.ubisoft.com/en > <i>Prince of Persia</i> is an action adventure online videogame. ⁷⁵⁰	Renne, France Montreal, Canada	'laws of England' Terms of Use (Ubisoft) A terms of service or privacy policy was not located on Ubisoft Montreal website
<i>Heroes of the Storm</i>	Blizzard Entertainment < http://eu.blizzard.com/en-gb > Age restriction 13+ ⁷⁵¹ A MOBA game where two teams fight against each other with rotating heroes. ⁷⁵²	Irvine, California, United States	laws of France' Terms of Use (Blizzard Entertainment)
<i>League of Legends</i>	Riot Games < http://www.riotgames.com > Age restriction 14+ ⁷⁵³ A MOBA game where two teams compete to win by destroying the opponent's core structure. ⁷⁵⁴	West Los Angeles, California, United States	'laws of Ireland' Terms of Use (Riot Games)
<i>Clash of Clans</i>	Supercell < supercell.com/ > Age restriction 13+ ⁷⁵⁵ A MMO/MMOB (massively multiplayer online game) strategy videogame where players build their own villages by using resources obtained after attacking other player's villages. ⁷⁵⁶	Helsinki, Finland	If a resident of United States, any disputes 'shall be governed in all respects by California law' Terms of Service (Supercell) If a resident outside of United States, then any disputes 'shall be governed by the laws of Finland'
<i>Minecraft</i>	Mojang Age restriction 8+ ⁷⁵⁷	Stockholm	'The laws of Washington State.' Terms of Service (Mojang)
	Microsoft Corporation (Parent organisation Mojang) < https://www.microsoft.com/en-gb/servicesagreement/ > <i>Minecraft</i> is a sandbox game (as opposed to traditional mediums of game play, the player has open-ended choice	Redmond, Washington, United States	If the player resides in Europe and uses cost-free services, then laws of Washington apply. If the player is using paid services, then the country of habitual residence of the player to which Microsoft

⁷⁴⁹ <<https://www.commonsemmedia.org/game-reviews/prince-of-persia-the-forgotten-sands>> accessed 2 January 2017.

⁷⁵⁰ <<https://www.ubisoft.com/en-US/game/prince-of-persia/>> accessed 2 January 2017.

⁷⁵¹ <<https://www.commonsemmedia.org/game-reviews/heroes-of-the-storm>> accessed 2 January 2017.

⁷⁵² <<http://us.battle.net/heroes/en/>> accessed 2 January 2017.

⁷⁵³ <<https://www.commonsemmedia.org/game-reviews/league-of-legends>> accessed 2 January 2017.

⁷⁵⁴ <<http://euw.leagueoflegends.com/>> accessed 2 January 2017.

⁷⁵⁵ <<https://www.commonsemmedia.org/app-reviews/clash-of-clans>> accessed 2 January 2017.

⁷⁵⁶ <<http://supercell.com/en/games/clashofclans/>> accessed 2 January 2017.

⁷⁵⁷ <<https://www.commonsemmedia.org/game-reviews/minecraft>> accessed 2 January 2017.

	to play the game)allows players to build their own worlds by using blocks. ⁷⁵⁸		directs its services will apply
	4J Studios < minecraft.gamepedia.com/4J_Studios >	Dundee	The terms of service and privacy policy was not located on the website
<i>Pogo</i>	Electronic Arts < https://www.ea.com/en-gb > Age restriction 13+ ⁷⁵⁹ It is a free online games website that offers more than 100 games including puzzles and board games. ⁷⁶⁰	Redwood City, California, United States	For residents living in EEA, Switzerland, Brazil, Mexico or Russia, the laws of the resident country apply. If the resident lives in United States, Canada or Japan then the laws of the State of California apply – Terms of Use (Blizzard Entertainment)
<i>Candy Crush Saga</i>	King < https://king.com/ > Age restriction 13+ ⁷⁶¹ A free-to-play mobile game involving matching a puzzle of animated candies to ascend levels. ⁷⁶²	Dublin, Republic of Ireland	For residents of United States, laws of Delaware will apply. If a ‘Class Action Waiver’ is ruled enforceable then the laws of California will apply. For residents living outside United States, Malta and the laws of England will apply
	King Records < http://kingrecords.net/ >	Bunkyo, Tokyo, Japan	A terms of service or privacy policy was not indicated on the King records website

Table 5 sets out the 10 videogame websites selected for the multiple case study.

Preliminary observations include absence of age verification within the videogame website, which had to be confirmed from other independent websites. It was also

⁷⁵⁸ <<https://minecraft.net/en-us/>> accessed 3 January 2017.

⁷⁵⁹ <<https://www.commonsemmedia.org/app-reviews/pogo-games>> accessed 3 January 2017.

⁷⁶⁰ <<http://www.pogo.com/>> accessed 3 January 2017.

⁷⁶¹ <<https://www.commonsemmedia.org/app-reviews/candy-crush-saga>> accessed 3 January 2017.

⁷⁶² <<https://king.com/game/candycrush>> accessed 3 January 2017.

observed that, although a videogame may be registered in one country, it may be governed by the laws of another state.

5.4.1. Preliminary observations on the governing data privacy law

Table 5 above shows that the location of the registered headquarters of a company is not always the place of the governing data privacy law. For example, the corporate headquarters of *League of Legends* is in California and governed by the 'laws of Ireland'. This raises worrisome data privacy issues for children and their parents, who will have to independently work out which law applies and governs the terms of the privacy policy. This is important because different legislatures accord varying levels of data privacy protection.

In all the cases above, it was found that the governing law is contained in the 'terms of service' (TOS) sections rather than the online privacy policy document, without any indication that the reader should refer to the TOS. In other words, there is no cross-referencing. The TOS is generally across the sample a lengthy, legal and technically framed document, and the governing law is not prominently displayed. Children and their parents would find it particularly difficult to locate the governing law. Although it is typical in a legal contract to find the applicable governing law at the end of the contractual terms, this may not be well known to users of videogame websites and their parents. The issues surrounding the complexity of governing law will be examined in more detail further on (*see 6.2.3.1 & 6.6.2*). Another observation is the issue of lengthy and complex privacy policies, which will be discussed in further detail in Chapter 6 (*see 6.2.1, 6.6.2 & 6.6.1*).

5.4.2. Videogame privacy policies and the associated reading issues

Privacy policies have been criticised for their length and use of complicated legal and technical terms. According to Canada-based lawyer Jordan Nahmias,⁷⁶³ since privacy notices are meant for avoiding any liability they tend to be very long, complicated and legalistic, which means they are hardly ever read.⁷⁶⁴

Privacy policies are complicated, full of jargon and keep updating and changing frequently,⁷⁶⁵ making it difficult for users to keep pace with the updates. The FTC took notice of the fact that most privacy policies are written by someone with a legal background and at a college reading level,⁷⁶⁶ making it difficult for children to read and understand them.

In the recent U.S. Federal District court case, *Mortensen v Bresnan Communications LLC*,⁷⁶⁷ the court required companies to pay attention to what their privacy policies say and how they are presented to users; they should not ignore the interactions with multiple other parties which are unknown to the user and will be collecting their information.

⁷⁶³ Jordan Nahmias <<http://www.nahmiaslaw.com/about/>> accessed 21 March 2018.

⁷⁶⁴ Jordan Nahmias, 'The EULA: What It Does, How It Works (and, What Does EULA Even Mean?)' (Nahmiaslaw, 23 November 2011) <<http://www.nahmiaslaw.com/the-eula-what-it-does-how-it-works-and-what-does-eula-even-mean/>> accessed 16 May 2016; Aleecia M. McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2009) 4 I/S: A Journal of Law and Policy for the Information Society 543 <<http://www.is-journal.org/>> accessed 20 January 2016. About half of Canadian youth have never read privacy policies of the websites they visit. Costas Lambrinoudakis and Alban Gabillon, *Risks and Security of Internet and Systems* (Springer 2015).

⁷⁶⁵ Lorrie Faith Cranor, 'Necessary but Not Sufficient: Standardised Mechanisms for Privacy Notice and Choice' (2012) 10 J. on Telecomm. & High Tech L. 273; Regina Saskatchewan, 'Resolution of Canada's Privacy Commissioners and Privacy Oversight Officials' (Office of the Privacy Commissioner of Canada, 4 June 2008) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_080604/?wbdisable=true> accessed 22 February 2018.

⁷⁶⁶ #339: Project No. P104503; 16 C.F.R. Part 312; Public Comment(s) on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act (COPPA) through the Children's Online Privacy Protection Rule (COPPA Rule) (Federal Trade Commission) <<https://www.ftc.gov/policy/public-comments/2013/08/initiative-339>> accessed 22 February 2017.

⁷⁶⁷ *Mortensen v Bresnan Communications CV 10-13-BLG-RFC* (D.Mont. Nov. 15, 2010).

These sections have explained the choice of 10 videogames; the legislation in the U.S., the EU and Canada; and the criteria for analysing privacy policies. The following sections will carry out the first part of the multiple case study, evaluating privacy policies using 11 criteria.

5.5. Evaluation of the privacy policies of 10 videogame websites selected for this thesis

In the forthcoming tables, each criterion listed in Table 4 will be compared against the privacy policies of each videogame listed in Table 5. This will be followed by analysing the stages of subscription of the games as it is the first point of consent between the website and players before they can become a member. It is important to study the stages of subscription, if any, to determine the kind and extent of personal information expected of children to submit.

In Table 6, the first criterion set out in Table 4, namely 'location of privacy policy', is analysed against each videogame.

5.5.1. Table 6 Criterion 1 – Location of privacy policy

Criterion 1 – Location of privacy policy
<i>Dota 2</i> – Privacy policy is not located on the main webpage but as a mandatory consent document before the login webpage
<i>Clash of Clans</i> – The policy was located at the bottom of the main webpage
<i>Miniclip</i> – The policy was located at the bottom of the main webpage
<i>Prince of Persia</i> – The policy was located at the bottom of the main webpage
<i>Heroes of the Storm</i> – The policy was located at the bottom of the main webpage
<i>League of Legends</i> – The policy was located at the bottom of the main webpage
<i>Minecraft</i> – The policy was located at the bottom of the main webpage
<i>Pogo</i> – The policy was not located on the main webpage but in the middle of the registration page
<i>Candy Crush Saga</i> – The policy was located at the bottom of the main webpage
<i>Princess Isabella</i> – The policy was located at the bottom of the main webpage

5.5.1.1. Is the privacy policy clearly distinguished from the rest of the webpage?

Links to nine privacy notices were located obscurely at the bottom of the main homepage and lacked any distinguishing features such as a different font colour and/or size. Only Pogo presented its privacy notice in the middle of the page.

Website operators have breached their legal obligation to post privacy notices prominently and facilitate children with easy accessibility. These legal requirements will be dealt with in Chapter 6: evaluating the second part of the multiple case study.

5.5.2. Table 7 Criterion 2 – Length and wording of the privacy policy

Criterion 2 – Length and wording of the privacy policy
<i>Dota 2</i> – 1,867 words ⁷⁶⁸
<i>Clash of Clans</i> – 3,422 words ⁷⁶⁹
<i>Miniclip</i> – 1,988 words ⁷⁷⁰
<i>Prince of Persia</i> – 5274 words
<i>Heroes of the Storm</i> – 2551 words
<i>League of Legends</i> – Expanded version 5058 words, collapsed version 2,806 words ⁷⁷¹
<i>Minecraft</i> – Expanded version 23,127 words, collapsed version 2,360 words ⁷⁷²
<i>Pogo</i> – 3,756 words ⁷⁷³
<i>Candy Crush Saga</i> – 4,809 words ⁷⁷⁴
<i>Princess Isabella</i> – 2,780 words

5.5.2.1. The length of the privacy policy

The length of the document, vagueness of the wording, legalistic and computer jargon, was another issue encountered during the study. The policies were regarded on two separate occasions, before and after 1 January 2017. They were updated in 2017, apart from *Heroes of the Storm*, which was updated on 5 July 2010⁷⁷⁵ and *Prince of Persia* was updated on 12 January 2016.⁷⁷⁶ The policies had made common

⁷⁶⁸ https://store.steampowered.com/privacy_agreement/ accessed 16 May 2018. The privacy policy of Dota 2 was revised on 23 January 2018. It does not exhibit any changes.

⁷⁶⁹ <http://supercell.com/en/privacy-policy/> accessed 16 May 2018. Clash of Clans will update its privacy policy on 25 May 2018. It will reduce the word length to 1608 words, introduce a table of contents and a separate guide to advise parents on children's in-game purchasing.

⁷⁷⁰ <https://www.miniclip.com/games/page/en/privacy-policy/> accessed 16 May 2018. The privacy policy of Miniclip was updated on 14 September 2017. The word count was increased to 2404 words.

⁷⁷¹ <https://na.leagueoflegends.com/en/legal/privacy> accessed 16 May 2018. The privacy policy was revised on 16 May 2018 without any distinct changes.

⁷⁷² <https://privacy.microsoft.com/en-us/privacystatement> accessed 16 May 2018. Microsoft's privacy policy was updated in April 2018. The expanded version is increased to 25708 words. The collapsed version is 2114 words.

⁷⁷³ <http://www.addthis.com/privacy/privacy-policy> accessed 16 May 2018. The privacy policy was updated on 7 September 2017 and the word limit was reduced to 3271 words.

⁷⁷⁴ <https://king.com/privacyPolicy> accessed 16 May 2018. The privacy policy was updated on 24 April 2018. The expanded version comprised of 6627 words. The collapsed version comprises of 1272 words.

⁷⁷⁵ < <http://eu.blizzard.com/en-gb/company/about/privacy.html> > accessed 16 May 2018.

⁷⁷⁶ <<https://legal.ubi.com/privacypolicy/en-US>> accessed 11 December 2017.

changes with regards to the wording and length. Previously, the word limit was between 10,000 and 15,000 words and on 1 January 2017 the word limit was 4,000 words. The websites have not provided any reason for the changes made. Journal articles were covered, updates on the [British and Irish Legal Information Institute \(BAILII\)](#) website and videos of conferences on children's digital privacy rights that took place in 2017 were regarded. The Information Commissioner's Office (ICO) was contacted with respect to the update of the privacy policies but it didn't respond. This is an outstanding question that has yet to be determined. It is speculated that the changes could have been instigated to initiate compliance with the EU GDPR 2018 which became effective on 25th May 2018.⁷⁷⁷

The EU GDPR 2018 requires companies to reconcile their practices with the law or incur hefty penal sanctions. The changes may also be attributed to the annulment of the Safe Harbour Principles by the European Court of Justice.⁷⁷⁸ It was found that U.S. companies were not providing adequate protection to data that was transferred from the EU. The Privacy Shield Framework was adopted five months afterwards, on 12 January 2017, to ensure safety for transfer of data from EU to the U.S.⁷⁷⁹

Dota 2 had the shortest privacy policy, with a word limit of 1,867 words, whereas *Minecraft's* expanded version was the longest at a remarkable 23,127 words. One of the issues associated with the word count was that there was no indication of the

⁷⁷⁷ 'The History of the General Data Protection Regulation' (Europa) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 11 December 2017.

⁷⁷⁸ Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid' (Europa, 6 October 2015) <http://curia.europa.eu/jcms/jcms/P_180250/> accessed 14 March 2017.

⁷⁷⁹ The Federal Council, 'Swiss-US Privacy Shield: Better Protection for Data Transferred to the USA' (The Federal Council) <<https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html>> accessed 14 March 2017.

number of words in the privacy policy and they had to be counted independently. Data privacy laws should provide word limits for children's privacy policies. Indication of a word limit in privacy policies will partly determine if they are child-friendly. Five out of 10 privacy policies expected players to read additional third-party privacy policies if they clicked on their links posted on the host website. This would significantly increase the number of words and the time taken to read them.

There is a significant reduction in the word limit but much more needs to be done because a 4,000-word document is still excessive. It constitutes eight A4 pages and is not compatible with the reading abilities of children. Children should not be expected to read third-party policies because the host website privacy policy will no longer apply. This effectively adds to the word length of the privacy policies that children are expected to read which is clearly contrary to the aim of treating children as a special class of data subjects.

Reflection on privacy policies updated in 2017/18

Six privacy policies studied were updated in late 2017 and 2018.⁷⁸⁰ This is likely due to preparing for implementing the EU GDPR 2018. The updated privacy policies did not exhibit any distinctive features. Some videogame privacy policies featured a table of contents, presumably in response to the EU GDPR 2018.⁷⁸¹ For the first time, the

⁷⁸⁰ <<http://supercell.com/en/privacy-policy/>> accessed 16 May 2018. The privacy policy of Clash of Clans was updated on 25th May 2018; < <https://www.miniclip.com/games/page/en/privacy-policy/>> accessed 16 May 2018. The privacy policy of Miniclip was updated on 14 September 2017; <https://privacy.microsoft.com/en-us/privacystatement> accessed 16 May 2018. Minecraft privacy statement was updated in April 2018; <https://euw.leagueoflegends.com/en/legal/privacy> accessed 16 May 2018. League of Legends privacy policy was updated on 16 May 2018; https://store.steampowered.com/privacy_agreement/ accessed 16 May 2018. The privacy policy of Dota 2 was revised on 23 January 2018; <https://king.com/privacyPolicy> accessed 16 May 2018. The privacy policy of Candy Crush Saga was updated on 24 April 2018.

⁷⁸¹ League of Legends; Minecraft; and Heroes of the Storm; No reason was provided for the update. It is speculated this could be done to show compatibility with the EU GDPR 2018.

updated policies describe the website's data handling practices regarding children in a separate paragraph.⁷⁸² Typically parents are advised to supervise children's online activities, that children under 13 years should furnish parental consent, and parents/legal guardians can contact the website to amend their children's data. Secondly, 6 videogame privacy policies have begun to treat children as a special class of data subjects by providing a separate children's privacy policy that deals with children's data gathering practices.

The word length has changed for the 6 privacy policies updated in late 2017 and 2018. Whereas Clash of Clans has reduced the word length from 3422 to 1608 words; Candy Crush Saga has increased its expanded word length to 6627 words; Minecraft has also increased its expanded word length to 25708. Although the privacy policies introduce a table of contents at the beginning of the document for easier readability, the increased word count lengthens the document. The EU GDPR 2018 requires website operators to clearly explain their data handling practices. The use and function of different kinds of cookies must be explained in simple terms⁷⁸³ (5.5.8.1). Therefore, the privacy policies are obliged to explain all the cookies used in their website which has added to the word count. The requirement to define cookies and explain their functions provide useful information to data subjects, but the resulting excessive content makes privacy policies onerous to read for children. EU GDPR 2018 should provide separate requirements for children's privacy policies. Cookies should be dealt with briefly and explained in easy to understand language.

⁷⁸² Candy Crush Saga; Dota 2; Princess Isabella; League of Legends; Miniclip; Clash of Clans.

⁷⁸³ EU GDPR 2018 Recital 29 and 30.

5.5.2.2. Typical structure of a videogame privacy policy

All the policies were set up in an organised structure listing data that can be collected by the website, along with how and why the data is collected and the sharing of the information with third parties. At the end, the policy described the rights of users, the complaints process and methods of dispute resolution. Pogo and *Clash of Clans* went a step further by explaining the reason behind the existence of the policy. Pogo defined personal data, non-personal data and cookies with simple examples that would be easier to understand. Such practice was not observed in other policies.

The privacy policy stated that the simple act of entering the website or using the service meant users had furnished consent and they were bound by the terms of the policy. Children and their parents were not given the option to accept or even question the policy. The privacy policies had a separate paragraph to guide parents about children's privacy. There was no distinction between the player and the parent and in most cases referred to players simply as 'you'. The divide between the responsibilities of the parent and child were not clearly laid out.

The gaming websites portrayed moderate complexity in the structuring of sentences, use of vocabulary and the formal style of writing. Difficult terms were also employed such as 'media access control' (MAC) and 'international mobile equipment identity' (IMEI)⁷⁸⁴ but did not explain their meaning. Policies were not able to explain such terms as 'the information will be kept for as long as is reasonably necessary'. What is

⁷⁸⁴ *Clash of Clans*.

meant by reasonable belief in this context? It is a broad term and can encompass a plethora of possibilities.

Five websites were targeted towards children above 13 years of age; one at seven-year-olds; one at eight-year-olds; one at ten-year-olds; one at 11-year-olds; and one at 14-year-olds. None of the policies was presented in child-friendly language or contained a separate policy specifically for children. The privacy policy of *League of Legends* and *Minecraft* provided a brief portion of each paragraph which could be expanded to read on additional details. This was helpful as one could read the most important information from the short paragraph. But most times, it was found to be important to read the expanded version owing to important pieces of information contained within.

5.5.2.3. Readability of the privacy policy

Data protection and privacy laws have not mentioned the rules on the requirement of the privacy policies to facilitate readability by users. California's Attorney General has provided a guide regarding readability:⁷⁸⁵ that it should use plain, straightforward language, avoid technical or legal jargon, use short sentences,⁷⁸⁶ and contain graphics or icons for users to easily recognise privacy practices and settings.⁷⁸⁷ The Attorney General took notice of a readability standard called the Flesch reading test,⁷⁸⁸ which is designed to indicate how difficult a passage in English is to understand.⁷⁸⁹ For

⁷⁸⁵ 'Making Your Privacy Practices Public' (California Department of Justice May 2014) <https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf> accessed 6 March 2017.

⁷⁸⁶ Ibid.

⁷⁸⁷ Ibid.

⁷⁸⁸ California Financial Information Privacy Act (Financial Code § 4053(d)).

⁷⁸⁹ Flesch Reading Ease Readability Formula (Readability Formulas)

<<http://www.readabilityformulas.com/flesch-reading-ease-readability-formula.php>> accessed 6 March 2017.

instance, a score of 50 or 'fairly difficult' is suitable for a tenth- to twelfth-grade student (16- to 18-year-olds) and a score of 70–60 for eighth- and ninth-grade students (13–15 years).⁷⁹⁰ *Dota 2* and *Clash of Clans* have an age restriction of 13+, so it is important that the policy is easily read by a 13-year-old child. It is advised that the privacy policy should use a test score of 100–90, or 'very easy to read'. This score is suitable for a grade 5 or 11-year-old child, which means that it uses easier sentences and avoids technical and legal jargon.

The players had to keep themselves informed of privacy policy updates and had to revisit the page from time to time to take account of any changes. Only Pogo stated that the player would be notified of any material changes via a notice on their homepage.

The updated policies on 1 January 2017 were still too long, expecting users to read third-party privacy policies. The simple act of entering would amount to acceptance of the policy by the user. Use of complicated language defeats the purpose of the policy to inform users of the website's data handling practices.

5.5.2.4. Children's understanding of legal consequences

Children between the ages of 16 – 17 years should not only be able to access, read and understand the privacy policy document; they should also be able to comprehend the legal consequences of providing consent. Children are often neglected as a group in legal research⁷⁹¹ and data protection and privacy laws do not

⁷⁹⁰ Ibid.

⁷⁹¹ Many medicines routinely used in children have not been formally evaluated by the system because the pharmaceutical industry is reluctant to study medicines in children. Sharon Conroy and others, *Drug Trials in Children: Problems and the Way Forward* (2000) 49(2) BJCP 93.

treat children as a special class of data subjects. There is limited research to understand whether children can appreciate the consequences of providing online consent; that their personal data will be collected, processed and potentially disclosed in accordance with terms of the privacy policy which is regulated by the governing data privacy law; and what rights and obligations they are entitled to under the governing data privacy law.

To understand this gap in knowledge, Dr Dawn Watkins has conducted a pioneering study to assess children's understanding of law through digital gaming.⁷⁹² The study involved children playing a videogame while being prompted to respond in certain situations and giving reasons for their choices. Such studies are valuable, since they make children an important part of the process, they give more accurate information about children's experiences and better resources that can help policymakers develop more efficient practices with relation to children.

Global Kids Online⁷⁹³ has identified that the available statistics and research literature provides uneven evidence on children's experience of internet use.⁷⁹⁴ It also provides that children's voices be heard, and their online experiences should form part of research projects alongside contributions from academics, governments, civil society

⁷⁹² Dawn Watkins and others, Exploring Children's Understanding of Law in Their Everyday Lives (2018) 38(1) Legal Studies; 'Assessing Children's Understanding of Law through Digital Gaming' (University of Leicester, 4 July 2014) <<https://www2.le.ac.uk/departments/law/news-events/law-news/assessing-children2019s-understanding-of-law-through-digital-gaming>> accessed 30 March 2018.

⁷⁹³ Global Kids Online in an international research project that collaborates with UNICEF, the London School of Economics and Political Science (LSE) and the EU Kids Online network to generate cross-national evidence around children's use of the internet. Global Kids Online <<http://globalkidsonline.net/>> accessed 25 April 2018.

⁷⁹⁴ Sonia Livingstone, 'A Method for Researching Global Kids Online – Understanding Children's Well-Being and Rights in the Digital Age' (Global Kids Online November 2016) <<http://globalkidsonline.net/>> accessed 25 April 2018.

and data industry experts.⁷⁹⁵ Children’s experiences are essential to improve policymakers’ understanding of children’s rights in the digital age.⁷⁹⁶

5.5.3. Table 8 Criterion 3 – Governing legislation

Criterion 3 – Governing legislation
<i>Dota 2</i> – It is governed by the laws of the State of Washington, USA
<i>Princess Isabella</i> – It is governed by the law of the State of Washington, USA
<i>Miniclip</i> – It is governed by the laws of England and Wales
<i>Prince of Persia</i> – It is governed by the laws of England
<i>Heroes of the Storm</i> – It is governed by the laws of France
<i>League of Legends</i> – It is governed by the laws of Ireland
<i>Clash of Clans</i> – It is governed by the laws of California and Finland
<i>Minecraft</i> – It is governed by the laws of State of Washington or country of habitual residence if the user resides outside Europe
<i>Pogo</i> – If the resident lives in USA/Canada/Japan, then the laws of California will apply otherwise the laws of the country of residence
<i>Candy Crush Saga</i> – For residents in the United States, laws of the state of Delaware will apply. If the users reside outside United States, then the laws of England will apply.

The evaluation of this criterion involves a legal analysis and is deemed to fit best in the next chapter (see 6.2.3 & 6.6.2), which will carry out a legislative investigation of the compatibility between the criteria established in *Table 4* and the data protection and governing data privacy laws.

Table 9 will analyse the fourth criterion, the Privacy Shield Framework, to safeguard the transfer of data between the EU and the U.S.⁷⁹⁷ The Directive requires that

⁷⁹⁵ Global Kids Online research toolkit – quantitative guide <<http://globalkidsonline.net/>> accessed 25 April 2018.

⁷⁹⁶ Ibid.

⁷⁹⁷ Alasdair Taylor, ‘International Transfers of Personal Data’ (Seqlegal, 20 January 2008) <<https://seqlegal.com/blog/international-transfers-personal-data>> accessed 15 March 2017.

member states should transfer data to a third country which ensures an adequate level of protection.⁷⁹⁸

When the Safe Harbour Scheme was declared invalid by the European Court of Justice,⁷⁹⁹ it was replaced with the EU–U.S. Privacy Shield⁸⁰⁰ Applying the Privacy Shield is voluntary, making it unnecessary for organisations to comply with it.⁸⁰¹ An organisation that complies with the Privacy Shield will have to inform individuals about its participation by providing a link or web address for the Privacy Shield List.⁸⁰²

⁷⁹⁸ Directive 95/46/EC Article 25(1).

⁷⁹⁹ European Commission, '2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)' (Europa) <<http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520>> accessed 14 March 2017; Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid' (Europa, 6 October 2015) <http://curia.europa.eu/jcms/jcms/P_180250/> accessed 14 March 2017.

⁸⁰⁰ European Commission, 'The EU-U.S. Privacy Shield' (Europa) <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> accessed 14 March 2017; The Federal Council, 'Swiss-US Privacy Shield: Better Protection for Data Transferred to the USA' (The Federal Council) <<https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html>> accessed 14 March 2017. On January 12, 2017, the Swiss government announced the approval of the Swiss–U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States.

⁸⁰¹ 'EU-U.S. Privacy Shield Framework Principles Issued by the US Department of Commerce (Europa) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf> accessed 14 March 2017.

⁸⁰² Privacy Shield Principles Notice 1(a)(i) <Privacy Shield Principles Notice 1(a)(i) <<https://www.privacyshield.gov/article?id=1-NOTICE>> accessed 14 March 2017.

5.5.4. Table 9 Criterion 4 – Privacy rules involving the Privacy Shield Framework to safeguard transfer of data between the EU and the U.S.

Criterion 4 – Privacy rules involving the Privacy Shield Framework to safeguard the transfer of data between the EU and the U.S.
<i>Dota 2</i> – It complies with the Privacy Shield Framework
<i>Clash of Clans</i> – It does not mention privacy rules
<i>Miniclip</i> – It does not mention privacy rules
<i>Prince of Persia</i> – It does not mention privacy rules
<i>Heroes of the Storm</i> – It does not mention privacy rules
<i>League of Legends</i> – It does not apply the EU–U.S. Privacy Shield and/or the Swiss–U.S. Privacy Shield
<i>Minecraft</i> – It does not mention privacy rules
<i>Pogo</i> – It complies with the EU–U.S. Privacy Shield Framework
<i>Candy Crush Saga</i> – It does not mention privacy rules
<i>Princess Isabella</i> – It complies with the EU–U.S. Privacy Shield Framework and the Swiss–U.S. Privacy Shield

The criteria for applying the framework are unclear so it is sensible to assume that games registered in the U.S. could implement it. But, since it holds voluntary status, companies may not feel compelled to use it. Only three out of a possible seven videogames have applied the framework. The entrance requirements are questionable. Will a company registered in the U.S. and governed by EU and U.S. laws (Pogo) apply the framework?

The privacy policy contains a Privacy Shield icon that can be clicked to open the Privacy Shield homepage. It contained numerous documents including the Privacy Shield Principles, which is a lengthy (36 pages)⁸⁰³ legal document. People with a non-legal background will find it exceptionally challenging to read and understand such

⁸⁰³ Privacy Shield Principles
 <<https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>> accessed 6 April 2018.

onerous documents. Additionally, it is not clear why they should even go through the principles.

Inclusion of the Privacy Shield Framework can be a good indicator to other businesses in commerce about the website's data handling practices, but it only complicates matters for children. Its voluntary status and unclear application have been questioned by the authorities (*see* 3.2.6).

The European Data Protection Supervisor has called for the Privacy Shield to be effective in providing adequate protection against indiscriminate surveillance as well as obligations on oversight, transparency, redress and data protection rights.⁸⁰⁴

Table 10 analyses the fifth criterion, TRUSTe Privacy Certification, which is an independent self-regulating online seal programme.⁸⁰⁵ It ensures websites are complying with certain privacy practices,⁸⁰⁶ which can be evidenced with a seal displayed on the website.⁸⁰⁷

⁸⁰⁴ European Data Protection Supervisor, 'Privacy Shield: More Robust and Sustainable Solution Needed' (Europa, 30 May 2016)

<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 14 March 2017.

⁸⁰⁵ 'Self-Regulation and Privacy Online' (Federal Trade Commission July 1999)

<<https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-online-federal-trade-commission-report-congress/1999self-regulationreport.pdf>> accessed 14 March 2017; Henry H. Perritt, Jr. 'Law and the Information Superhighway' (2nd edn. Aspen Law and Business 2001) The TRUSTe is an independent for-profit organisation.

⁸⁰⁶ TRUSTed websites privacy certification (TRUSTe) <<https://www.trustarc.com/privacy-certification-standards/>> accessed 14 March 2017. The website should be adopting and implementing a privacy policy; posting notice and disclosing collection and use practices; giving users choice and consent over how their personal information is used and shared; and implementing data security, quality and access measures.

⁸⁰⁷ Jacqueline Klosek, *Data Protection in the Information Age* (Quorum Books 2000); 'Self-Regulation and Privacy Online' (Federal Trade Commission July 1999) <<https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-online-federal-trade-commission-report-congress/1999self-regulationreport.pdf>> accessed 14 March 2017. According to the FTC, seal programs offer an easy way for website users to determine whether the website complies with specified information practice principles.

5.5.5. Table 10 Criterion 5 – TRUSTe privacy certification

Criterion 5 – TRUSTe privacy certification
<i>Dota 2</i> – It does not apply TRUSTe Privacy Certification
<i>Clash of Clans</i> – It applies the TRUSTe Privacy Certification
<i>Miniclip</i> – It does not apply TRUSTe Privacy Certification
<i>Prince of Persia</i> – It does not apply TRUSTe Privacy Certification
<i>Heroes of the Storm</i> – It does not mention the TRUSTe Privacy Certification
<i>League of Legends</i> – It applies the TRUSTe Privacy Certification
<i>Minecraft</i> – It does not mention the TRUSTe Privacy Certification
<i>Pogo</i> – It applies the TRUSTe Privacy Certification
<i>Candy Crush Saga</i> – It does not mention the TRUSTe Privacy Certification
<i>Princess Isabella</i> – It does not mention the TRUSTe Privacy Certification

Two out of 10 websites adhere to TRUSTe but without any explanation for its presence. A logo can be clicked to access the homepage of TRUSTe. The webpage contains a paragraph that TRUSTe helps to certify company’s privacy practices, followed by a table containing five certification standards. One of the standards is titled ‘Children’s Privacy’, which is a 31-page document aimed at websites rather than users and provides information for businesses to comply with TRUSTe practices.⁸⁰⁸

The information is suited for businesses in commerce rather than children and/or their parents and therefore should be avoided in children’s privacy policies. Such frameworks have been criticised for their unclear purpose and eligibility criteria, voluntary status and the expectation from users to click on links that will take them

⁸⁰⁸ <<https://www.trustarc.com/privacy-certification-standards/>> accessed 13 February 2017; European Commission, EU-U.S. Privacy Shield (Europa) <[http://Europa.eu/rapid/press-release MEMO-16-434_en.htm](http://Europa.eu/rapid/press-release_MEMO-16-434_en.htm) accessed 13 February 2017>; EU-US Privacy Shield Solutions (TRUSTe) <<https://www.truste.com/business-products/dpm-services/eu-privacy-shield/>> accessed 13 February 2017.

to the homepage, where they have to explore and understand the rules for themselves.

Table 11 below analyses the sixth criterion, 'collection of information from videogame website users'. The table will quantify the pieces of information collected by the website to examine the notion that website operators build an extensive personal profile of the user.⁸⁰⁹ Collecting personal data helps the company improve understanding of their player demographics and increase the popularity of the game. For instance, *Candy Crush Saga* (Chapter 5 Table 5) noticed that users of the free mobile app would quit the game around Level 65 because the game became very hard to play. Level 65 was made easier to allow users to progress further into the game.⁸¹⁰

⁸⁰⁹ 'Video Game Companies Are Collecting Massive Amounts of Data about You (thestar.com) <<https://www.thestar.com/news/canada/2015/12/29/how-much-data-are-video-games-collecting-about-you.html>> accessed 15 March 2017.

⁸¹⁰ Ibid.

5.5.6. Table 11 Criterion 6 – Collection of information from children

Videogame websites	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7	Group 8	Total no. of data collected
<i>Dota 2</i>	✓	✓	✓			✓		✓	9
<i>Clash of Clans</i>	✓		✓	✓	✓	✓	✓		21
<i>Candy Crush Saga</i>	✓		✓	✓	✓	✓	✓		7
<i>Heroes of the Storm</i>	✓	✓	✓		✓	✓	✓		12
<i>League of Legends</i>	✓	✓	✓	✓	✓	✓	✓	✓	28
<i>Princess Isabella: A Witch's Curse</i>	✓	✓	✓	✓	✓	✓	✓	✓	17
<i>Pogo</i>	✓	✓			✓	✓	✓	✓	26
<i>Miniclip</i>	✓			✓	✓	✓	✓	✓	23
<i>Prince of Persia</i>	✓		✓		✓			✓	26
<i>Minecraft</i>	✓		✓	✓	✓	✓	✓		36

The law relating to personal data will be discussed in more detail in *Chapter 6*. In this section it will be considered whether such practices remain in the best interests of children. The information collected is classed into eight broad separate groups. These groups are based on the types of personal data that will be collected by the videogame websites selected for this study.

Group 1 contains users' names, passwords, email addresses, postal addresses, genders, dates of birth and telephone numbers. Group 2 contains credit card information, credit card expiry dates and billing addresses. Group 3 shows data about

users' interests and preferences, information about how users interact with the websites, information that helps secure access to the websites' services, use of website services such as browsing time, searches, scrolling and in-game interactions. Group 4 includes IP (internet protocol) addresses. Group 5 includes device names, hardware types, versions of individuals' operating systems (OS), unique device IDs (persistent/non-persistent). Group 6 includes MAC addresses, IMEIs, ISPs (internet service providers), preference settings and software used such as browser type. Group 7 shows geographic location and language preferences. Group 8 includes information about website performance and problems users may encounter.

5.5.6.1. Distinction between personal information and non-personal information defined

The privacy policies (apart from Pogo) did not make a clear distinction between 'personally identifiable information' and 'non-personally identifiable information'. . According to Article 4 EU GDPR, 'personal data' means any information relating to an identified or identifiable natural person. The distinction between personal and non-personal data is important because if data falls in the former category, it is protected by privacy law. Therefore, non-personal data will not be protected by law. However, in October 2016, the European Court of Justice ruled in *Patrick Breyer v Bundesrepublik Deutschland*⁸¹¹ that dynamic IP addresses will constitute personal data because they will comprise a 'means likely reasonably to be used to identify' the individual.⁸¹² Although dynamic IP address is per se is not sufficient to identify the

⁸¹¹ [Judgment in Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland.](#)

⁸¹² Ibid.

individual, but according to the ECJ it is personal data because it can be used alongside other information to identify an individual. This is a broad interpretation by the ECJ, aligned with a possible trend to broaden the scope of personal data. Hence, it is helpful if website operators acknowledge the fact that non-personal data can be used alongside personal data to identify an individual. This approach has been adopted in Hilton Hotel & Resorts⁸¹³ global privacy policy published on 14 November 2017.⁸¹⁴ A global privacy policy is an example of good practice where organisations operate in multiple jurisdictions. Under the section titled 'Other information', it is said that non-personal information doesn't identify the user and can be disclosed for any purpose permitted by law. But it also states that the website may combine such information with personal data, in which case it will be treated as personal information.

Apart from *Prince of Persia*, none of the games accepted the possibility that non-personal data could become personal data. Legislators need to rethink the distinction between personal and non-personal information and the ability of the latter to become the former.⁸¹⁵

It is recommended that website privacy policies should inform the user that if non-personal data is combined with personal information it will be treated as personal data. This is in accordance with the EU GDPR 2018 which recognises that online

⁸¹³ Hilton <<http://www3.hilton.com/en/index.html>> accessed 20 April 2018. Hilton Hotel & Resorts is a global brand of full-service hotels under the Hilton brand.

⁸¹⁴ Hilton Honors <<http://hiltonhonors3.hilton.com/en/policy/global-privacy-statement/index.html>> accessed 20 April 2018.

⁸¹⁵ See Chapter 6 – Compatibility of videogame case study with the governing data privacy law.

identifiers (IP Address, E-mail address etc) can be combined with other information to identify natural persons.⁸¹⁶

No uniform term applied to describe 'non-personal information'. *Prince of Persia* used the word 'passive collection', whereas *Princess Isabella* called it 'other information'. The lack of clear distinction or explanation between personal and non-personal data appears to treat all the data as personal data.

5.5.6.2. Was consent needed to authorise collection and processing of user data?⁸¹⁷

Directive 95/46/EC required 'unambiguous consent' from the data subject⁸¹⁸ which was defined as 'any freely given specific and informed indication of his wishes'.⁸¹⁹

Consent should empower the data subject to make conscious, rational and autonomous choices in relation to the processing of their personal data.⁸²⁰ Children and their parents should understand and appreciate the implications of giving consent.⁸²¹ In reality, consent is not a positive and informed action on the part of the user. Some privacy policies are implying consent when the user accesses the website or uses its services. If users click on a link contained within the website and access a third-party website, they would have impliedly consented to the data handling practices of the third-party website. This means that children are unknowingly furnishing consent and allowing website operators to collect, process and disclose

⁸¹⁶ EU GDPR 2018 Recitals 26 and 30.

⁸¹⁷ *Chapter 4 Section 4.10.3*

⁸¹⁸ Directive 95/46/EC Article 7(a); EU GDPR 2018 Article 4(h) and 7.

⁸¹⁹ Directive 95/46/EC Article 2(h).

⁸²⁰ Bart W. Schermer, Bart Custers and Simone Van Der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) *Ethics Info Technol* 171.

⁸²¹ *Ibid.*

their personal data to third parties. Consent is not an autonomous, unambiguous, informed or conscious choice representing the user's wishes.

5.5.6.3. Websites collect extensive information from users

Table 11 represents the extensive information collected from users, infringing the principle of minimality,⁸²² which requires that data collection be limited to the purpose for which it was collected. The collection of the information goes beyond the information required to register for the account such as usernames, email addresses etc. In some instances, the operator also required the users' first and last names and will tap into the users' hardware, software, browser type and system, files containing documents, photos, contacts (*Minecraft*), chat messages, social media accounts etc. The surveillance became very invasive as it built a detailed profile of the user, detailing their hobbies and interests. It is unclear how this information would satisfy the legal requirement for legitimate processing and collecting adequate and not excessive data.

Privacy policies used vague purposes for collection such as 'improving user experience' (see 3.2.3.2), which have been rejected by the Art29 WP for their unclear meaning.⁸²³

All websites collected information related to the user's browser. For instance, Pogo and *Prince of Persia* collected the players' IP addresses, mobile and other hardware or device identifiers, platform types, browser information, hardware and software, operating systems, MAC addresses etc. According to *Princess Isabella and the Witch's*

⁸²² Directive 95/46/EC Article 6(1)(c); EU GDPR 2018 Article 5(c).

⁸²³ Ibid.

Curse, 'We may also track other types of information, such as what games users download and install, any download errors, what game users purchase'. This is not an exhaustive list. The language employed in the policy is vague and susceptible to different interpretations. It is not clear what hardware and software is being monitored and why. It is not mentioned whether the scrutiny is limited to the use of the game by the player's browser or whether it goes beyond the use of that particular game. The collection of data from the user's software applications installed on the machine could be interpreted to mean the ability of the games website to monitor any program installed on the player's PC and mobile device. It could also mean that the privacy policy grants permission to the website to scrutinise programs that users have installed and uninstalled on their computers, which could allow access to individuals' Windows logs as well. This can be a serious intrusion into one's privacy.

Microsoft collects usage data relating to the way the user and the device interact with Microsoft and its products. This can include voice interactions with Cortana.⁸²⁴ To enable Cortana,⁸²⁵ Microsoft collects extensive information from users⁸²⁶ giving rise to privacy issues.

The updated privacy policies have removed the term 'implied consent' from their privacy policies. According to the EU GDPR 2018, consent should be a positive and affirmative action on the part of the user and data subjects should have the option to withdraw consent at any time.⁸²⁷ Four privacy policies are implying consent and

⁸²⁴ 'What Is Cortana' (Microsoft) <<https://support.microsoft.com/en-gb/help/17214/windows-10-what-is> accessed 9 October 2016>. Cortana assists the user by providing reminders based on time, places or people etc.

⁸²⁵ <[https://en.wikipedia.org/wiki/Cortana_\(software\)](https://en.wikipedia.org/wiki/Cortana_(software))> accessed 9 October 2016.

⁸²⁶ 'Cortana and Privacy' (Microsoft) <<https://privacy.microsoft.com/en-US/windows-10-cortana-and-privacy>> accessed 9 October 2016.

⁸²⁷ EU GDPR 2018 Article 3.

the updated privacy policies are still collecting extensive information from children. This is not compatible with the EU GDPR 2018 which requires website operators to comply with data minimisation and purpose limitation.

5.5.6.4. Fears about websites collecting children's information

The policies state that they collect the content of chat messages. Children conveniently reveal personal information when participating in chat rooms and on social media or when they are posting messages to their friends. During the multiple case study of *Clash of Clans* (Table 3), users in public chat rooms revealed their genders, names, mobile numbers, and cities/countries of residence.

With prevailing data privacy risks, website operators should be very careful when collecting information from children. If the website's secure servers were disabled for some reason and hackers were to attack them, they could be in possession of children's personal information and even get access to their personal computer, containing important private files.

Table 12 analyses the seventh criterion, third parties collecting information from users of websites. A third party has been defined by Directive 95/46EC as any entity other than the data subject, the controller and the processor authorised to process the data.⁸²⁸

⁸²⁸ Directive 95/46/EC Article 2(f): In identifying the purposes, processing of data can occur for the legitimate interests pursued by the controller or third party except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection. Article 7(f) Directive 95/46/EC. CalOPPA requires website operators to disclose if any third parties are collecting personal information. CalOPPA 22575(b)(6). 'Complying with COPPA: Frequently Asked Questions' (Federal Trade Commission) <<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Disclosure>> accessed 16 March 2017. COPPA advises businesses to ensure that third parties' data privacy practices maintain the confidentiality and security of data and prevent unauthorized access and use of the information.

5.5.7. Table 12 Criterion 7 – Third parties collecting personal information

Criterion 7 – Third parties collecting personal information
<i>Dota 2</i> – ‘Third party publishers may also collect personally identifiable information as a requirement of accessing their games or content’ ⁸²⁹
<i>Clash of Clans</i> – ‘Our services may contain third party tracking tools to enable them to collect and analyze user information on our behalf’ ⁸³⁰
<i>Miniclip</i> – ‘Third party companies ... may ask for information from you which would be governed by the privacy policy of such companies’ ⁸³¹
<i>Prince of Persia</i> – ‘We may obtain certain information about you from third parties, including Personal Information’
<i>Heroes of the Storm</i> – ‘we may divulge this data to third party vendors in response to a product order or to add you to a vendor’s commercial bulletin circulation list’ ⁸³²
<i>League of Legends</i> – ‘We work with third parties to make your experience better ... There are several ways you might share info with third-party websites or services in connection with your visit’ ⁸³³
<i>Minecraft</i> – ‘We share data we collect with third parties’ ⁸³⁴
<i>Pogo</i> – ‘We also may receive information from third parties to supplement the information we receive from you. We use information from these companies primarily to help us deliver relevant advertising to you’ ⁸³⁵
<i>Candy Crush Saga</i> – ‘We may also collect information from advertising platforms and partners and other third parties such as information about purchases and interests’ ⁸³⁶
<i>Princess Isabella</i> – ‘Web sites that link to or from a Big Fish Games Offering may collect personal information about you’ ⁸³⁷

5.5.7.1. User ceases protection of host website upon clicking a third-party link

Table 12 notes that all websites allow third parties to collect personal information from users. Once a third-party link on the host website is clicked, responsibility is

⁸²⁹ Valve Privacy Policy <http://store.steampowered.com/privacy_agreement/> accessed 15 March 2017.

⁸³⁰ Supercell Privacy Policy <<http://supercell.com/en/privacy-policy/>> accessed 15 March 2017.

⁸³¹ Miniclip Privacy Policy <<http://www.miniclip.com/android/privacy-policy/>> accessed 15 March 2017.

⁸³² Blizzard Privacy Policy <<http://eu.blizzard.com/en-gb/company/about/privacy.html>> accessed 15 March 2017.

⁸³³ Riot Games Privacy Policy <<http://euw.leagueoflegends.com/en/legal/privacy#expand>> accessed 15 March 2017.

⁸³⁴ Microsoft Privacy Policy <<https://privacy.microsoft.com/en-us/privacystatement>> accessed 15 March 2017.

⁸³⁵ Electronic Arts Inc. Privacy Policy <<http://www2.ea.com/privacy-policy>> accessed 15 March 2017.

⁸³⁶ King Privacy Policy <<http://about.king.com/consumer-terms/terms/en>> accessed 15 March 2017.

⁸³⁷ Big Fish Games, Inc. Privacy Policy <<http://www.bigfishgames.com/company/privacy.html>> accessed 16 March 2017.

dismissed for the data collection practices of third-party advertisers, as users are encouraged to check the third party's privacy policies. Users are expected to determine for themselves if they are offered sufficient data privacy protection. This would be a particularly complex task for children. The host website should be responsible for ensuring that third-party advertisers remain compatible with acceptable privacy standards.

5.5.7.2. Ambiguous reasons provided for third parties collecting user information

The privacy policies give ambiguous reasons for allowing third parties to collect personal information. For example, in *Princess Isabella* 'third parties have access to your information only as necessary to perform their functions, and for no other purposes' and in *League of Legends* 'we work with third parties to make your experience better'. The terms 'necessary to perform functions' and to make the user's 'experience better' are difficult to stipulate and are not clearly explicit purposes to legitimise the collection of data (see 3.2.3.2).

The updated privacy policies have not clarified the role of third parties; their purpose behind data collection; and the kinds of data they collect. It is not compatible with the principles of data minimisation⁸³⁸ (see 3.2.3.3), transparency and purpose specification⁸³⁹ (see 3.2.3.2 & 3.2.4), and strict consent requirements under the EU GDPR 2018 (see 3.2.5.5 & 3.2.5.6) that ensures children's personal data remains safe.

⁸³⁸ Directive 95/46/EC Article 6(1)(c): The principle of minimality limits data collection to achieve the purpose behind the collection.

⁸³⁹ Directive 95/46/EC Article 6(1)(b): Under the principle of 'purpose specification', data should be gathered for a specified, legitimate and compatible purpose.

Table 13 will analyse the eighth criterion, cookies and other tracking technologies. New forms of user surveillance collect and process data to predict preferences and activities and share this information with third parties, who can then target commercial advertisements to these users.⁸⁴⁰ While the electronic content conducive for targeted advertisements is extremely important, they pose a risk to digital privacy. Technological advances such as cookies,⁸⁴¹ web beacons,⁸⁴² scripts⁸⁴³ and ad analytics⁸⁴⁴ are information-gathering, web-tracking tools that can facilitate the collection of personal information from online users easily, and in most instances without their knowledge.⁸⁴⁵

Also known as the HTTP cookie (hypertext transfer protocol),⁸⁴⁶ cookies are of different kinds including flash cookies.⁸⁴⁷ The persistent nature of flash cookies would make it exceptionally hard for children to attempt to delete them.

⁸⁴⁰ Julia Angwin and Tom McGinty, 'Sites Feed Personal Details to New Tracking Industry' *The Wall Street Journal* (30 July 2010) <<https://www.wsj.com/articles/SB10001424052748703977004575393173432219064>> accessed 18 March 2017.

⁸⁴¹ Cookies are small text files that are downloaded onto a user's computer or smartphone when they visit a website. It helps to remember users' devices as well as store information about their preferences or past actions 'Cookies and Similar Technology' (ICO) <<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>> accessed 18 March 2017.

⁸⁴² Web beacons, pixel tags or clear gifs are single-pixel graphics interchange format (GIF) that are bits of programming code included in web pages, emails and ads that notify the website when those web pages, emails or ads have been viewed or clicked on. 'Use of Cookies and Similar Technology' (Adobe, 16 June 2016) <<http://www.adobe.com/uk/privacy/cookies.html>> accessed 18 March 2017.

⁸⁴³ Scripts are also embedded within the website to measure how it is used and which links are clicked. Ibid.

⁸⁴⁴ Ad analytics use website analytic tools such as ad servers to quantify the effectiveness of digital advertising Wes Nichols, 'Advertising Analytics 2.0' (*Harvard Business Review*, March 2013) <<https://hbr.org/2013/03/advertising-analytics-20>> accessed 18 March 2017.

⁸⁴⁵ Janice C. Sipior, Burket T. Ward and Ruben A. Mendoza, 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons' (2011) 10(1) *Journal of Internet Commerce* 1.

⁸⁴⁶ HTTP cookies, commonly referred to simply as cookies, are small pieces of data sent from the website to the user's hard drive by the user's web browser to remember stateful information (such as items in a shopping basket); Mika D. Ayenson and others, 'Flash Cookies and Privacy II: Now with HTML5 and ET AG Respanning' (10 August 2009)

<https://webcache.googleusercontent.com/search?q=cache:4X55IK8ry_UJ:https://pdfs.semanticscholar.org/42cf/18892910afd15b0d6872f16384a7bb6cf915.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 18 March 2017.

HTTP cookies expire at the end of a web session, can be deleted and are easy to find.

⁸⁴⁷ J. Lott, D. Schall, and K. Peters, *Actionscript 3.0 Cookbook*, O'Reilly (2006) <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.7830&rep=rep1&type=pdf>> accessed 18 March 2017. Flash cookies can carry up to 100KB of information by default (HTTP cookies only store 4KB); Jeremy Kirk, 'Adobe Flash Cookies Pose Vexing Privacy Questions' (*Pcworld*, 11 August 2009)

It is necessary to analyse the tracking technologies used in videogame websites because of the inherent risk to online privacy. Does the privacy policy explain the use of tracking technologies and are users told the importance of changing their privacy settings?

5.5.8. Table 13 Criterion 8 – Cookies and other tracking technologies

Criterion 8 – Cookies and other tracking technologies
<p><i>Dota 2</i> – It uses cookies and other technologies such as web beacons and pixel tags (under section heading ‘Cookies and other information on a user’s machine’)</p> <p><i>Clash of Clans</i> – It uses cookies, beacons, scripts, tags and mobile analytics (under section heading ‘Tracking Technologies’ ‘Mobile Analytics’ ‘Third Party Services’)</p> <p><i>Miniclip</i> – It uses web analytics tools, such as Google Analytics, flash cookies, web beacons (under section heading ‘Information we collect’)</p> <p><i>Prince of Persia</i> – It uses cookies and other technologies (under section heading ‘Cookies’)</p> <p><i>Heroes of the Storm</i> – The policy uses cookies and other tracking technologies (under section heading ‘What cookies are and how we use them?’)</p> <p><i>League of Legends</i> – It uses cookies, web beacons, and other common tracking technologies (under section heading ‘Your choices and controls’)</p> <p><i>Minecraft</i> – Minecraft uses cookies, similar technologies and web beacons (under section heading ‘Cookies and similar technologies’)</p> <p><i>Pogo</i> – Pogo uses cookies and similar technologies, ad serving technologies that use cookies, clear GIFs, web beacons, tracking pixels, and other similar technologies like identifiers, internet log files, HTML 5 cookies, Silverlight Application Storage, device fingerprints and flash cookies (under section heading ‘Cookies and similar technologies’ ‘Analytics technologies’ ‘Ad serving technologies’)</p> <p><i>Candy Crush Saga</i> – It collects cookies and similar tracking technologies, analytic tools and mobile devices sometimes use advertising (or ad) identifiers (under section heading ‘How do ad identifiers, cookies and other similar technologies work?’)</p> <p><i>Princess Isabella</i> – The policy uses cookies (under section heading ‘Cookies’)</p>

<<http://www.pcworld.com/article/169985/article.html>> accessed 18 March 2017. Flash cookies are more persistent than HTTP cookies because HTTP cookies can expire at the end of a session, whereas flash cookies do not have expiration dates by default; flash cookies have the ability to recreate deleted HTTP cookies. Mika D. Ayenson and others, ‘Flash Cookies and Privacy II: Now with HTML5 and ET AG Respanning’ (10 August 2009) <https://webcache.googleusercontent.com/search?q=cache:4X55IK8ry_UJ:https://pdfs.semanticscholar.org/42cf/18892910afd15b0d6872f16384a7bb6cf915.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 18 March 2017. Browser controls do not delete flash cookies and they are stored in a different location. Ashkan Soltani and others, ‘Flash Cookies and Privacy’ (University of California) <<https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1070/1505>> accessed 20 September 2016. Users may not know what files to delete in order to eliminate them.

5.5.8.1. Failure to explain the different forms of tracking tools including flash cookies

All the videogames used a combination of tracking technologies. Although websites defined ‘cookies’, there was no explanation for the other tracking technologies used. Hilton Hotels’ global privacy policy has a separate document called ‘cookie statement’ and explains the different kinds of cookies used by the website.⁸⁴⁸ Information about tracking technologies was worded in subtle terms. There was no indication of the associated data privacy risks and that users were to adjust their privacy settings accordingly. Readers did not feel the need to alter their browser settings. According to the Information Commissioner’s Office guidelines, websites must explain how cookies work in clear terms, where users understand the consequences of cookies and the language level should be appropriate for the intended audience.⁸⁴⁹

Children’s privacy policies should refrain from using technical words that will need further explanation, elongate the document and unnecessarily complicate it. Instead, only one tracking technology (cookie) should be explained as representative of the rest. Users should also be told about the importance of altering privacy settings.

In the privacy policies updated in 2017/18, this position has changed. 4 out of 6 privacy policies⁸⁵⁰ explain cookies and other tracking technologies used by the website, in relatively simpler terms. The EU GDPR 2018 admits that online identifiers

⁸⁴⁸ Hilton Honors <<http://hiltonhonors3.hilton.com/en/policy/global-privacy-statement/index.html>> accessed 20 April 2018.

⁸⁴⁹ ‘Cookies and Similar Technologies’ (ICO) <<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>> accessed 19 March 2017.

⁸⁵⁰ *Minecraft, Candy Crush Saga, Dota 2 and League of Legends.*

such as cookies can uniquely identify natural persons, amounting to personal data.⁸⁵¹ This means that the use and functions of different kinds of cookies will have to be explained in a clear, intelligible and clear manner⁸⁵² for users to understand. This is a welcome change as children will be well-informed of the technologies used to gather their data. It is recommended that such information be provided in more succinct, brief and simple terms so that children don't feel burdened with additional information to read.

In Table 14, the ninth criterion, methods to disable cookies and other third-party tracking technologies will be discussed. Europa⁸⁵³ states that users should be allowed the option to disable cookies.⁸⁵⁴ Research conducted on the potential impact of cookie regulation found that respondents had limited understanding of cookies,⁸⁵⁵ with 37% of adults having no idea on how to manage them.⁸⁵⁶

The updated privacy policies⁸⁵⁷ define cookies in simpler words. Other similar technologies and tracking mechanisms have also been defined and their purpose explained to the user in relatively easier terms. The EU GDPR 2018 requires informing users of the website's tracking technologies, their purpose and functions. Some videogame websites are asking users to consent to privacy policies on the homepage. If users decline, they are removed from the website. This is contradictory to the

⁸⁵¹ EU GDPR 2018 Recital 29 and 30.

⁸⁵² EU GDPR 2018 Recital 58 and 60; EU GDPR 2018 Article 12.

⁸⁵³ 'Cookies' (Europa) <http://ec.europa.eu/jpg/basics/legal/cookies/index_en.htm> accessed 19 March 2017.

⁸⁵⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

⁸⁵⁵ 'Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework (Department for Culture, Media and Sport, April 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77641/PwC_Internet_Cookies_final.pdf> accessed 19 March 2017.

⁸⁵⁶ Ibid.

⁸⁵⁷ *Minecraft, Candy Crush Saga, Dota 2 and League of Legends.*

purpose of the EU GDPR 2018, which empowers users to choose to give consent and question the website’s data handling practices. Asking users to consent on the homepage is not giving them a choice but forcing them to consent.

5.5.9. Table 14 Criterion 9 – Methods to disable cookies and other third-party tracking technologies

Criterion 9 – Methods to disable cookies and other third-party tracking technologies
<p><i>Dota 2</i> – Users can consult their browser documentation to disable cookies</p> <p><i>Clash of Clans</i> – The user can opt out of behaviourally targeted advertising and analytics easily by accessing http://www.supercell.com/partner-opt-out and clicking opt-out.</p> <p><i>Miniclip</i> – Users can opt out of cookies by consulting their browser documentation. Users can also visit www.networkadvertising.org/choices/ to opt out of interest-based advertising.</p> <p><i>Prince of Persia</i> – The policy describes the method to disable cookies and tracking mechanisms. The user is advised to consult their browser documentation to alter cookie preferences, to read privacy policies of third parties to understand their use of cookies and to email https://legal.ubi.com/cookies to get a list of the companies uploading cookies on <i>Prince of Persia</i> and the means to opt out.</p> <p><i>Heroes of the Storm</i> – Users can consult their browser documentation to disable cookies</p> <p><i>League of Legends</i> – The user can consult browser documentation, opt out by following instructions in promotional emails. To opt out of third-party tracking mechanisms, users are required to visit http://www.aboutads.info or http://www.networkadvertising.org/choices</p> <p><i>Minecraft</i> – The policy requires users to opt out by clicking different links specifically dedicated to the opting out of different forms of tracking mechanisms. Once opened the documents are framed in difficult-to-understand English.</p> <p><i>Pogo</i> – Cookies can be disabled by referring to browser settings or adjust your preferences in the Macromedia Website Privacy Settings Panel at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html.</p> <p><i>Candy Crush Saga</i> – The user can adjust their preferences by consulting their browser or access different links in accordance with their country of residence where they access the services from</p> <p><i>Princess Isabella</i> – Users can adjust their preferences by consulting their browser and opt out of third-party ad serving cookies by clicking on www.networkadvertising.org/managing/opt_out.asp</p>

The mechanism to opt-out of cookies was dealt with in most privacy policies. Some policies⁸⁵⁸ provided a link with instructions that users could follow to disable cookies.

⁸⁵⁸ *Clash of Clans, Prince of Persia, Pogo, Miniclip, League of Legends and Princess Isabella.*

5.5.9.1. Complicated methods to opt out of tracking technologies

Another key finding of the study was that the method to opt out or disable cookies was complicated and difficult to follow. The opt-out method allows users to prevent websites from collecting their information and sending them with unsolicited product or service information. A link is clicked to open numerous technical documents with minimal instructions on the process to opt out (*Prince of Persia* and *Princess Isabella*). In some privacy policies (*Miniclip*), the reader is required to individually opt out of 79 companies (although this was not clearly stated as there was only a box to tick). In Pogo, the research could only progress with disabling cookies after downloading Flash Player. Absence of this software halted any further progress. At times the reader is met with the option to opt out of ‘interest-based advertising’, ‘online advertising’ and ‘cross-apps advertising’, with no explanation for these terms.

Websites expected users to consult their browser documentation and find out the procedure to disable cookies. According to David Wright and Reinhard Kreissl, players rarely or never adjust their browser settings,⁸⁵⁹ making it difficult for users to consult browser documentation. Many browsers such as Chrome and Internet Explorer have inbuilt security features which can be altered by the user.⁸⁶⁰ Some children may not have the requisite skills to operate privacy settings which makes it essential to publish a child-friendly privacy policy that contains simple instructions for parents and children aged 16 – 17 can follow and alter their privacy settings. It would be

⁸⁵⁹ David Wright and Reinhard Kreissl, *Surveillance in Europe* (Routledge 2015).

⁸⁶⁰ Nate Lord, ‘Browser Security Settings for Chrome, Firefox and Internet Explorer: Cybersecurity 101’ (Veracode, 22 March 2013) <<https://www.veracode.com/blog/2013/03/browser-security-settings-for-chrome-firefox-and-internet-explorer>> accessed 24 October 2016.

unreasonable for videogame websites to expect children to independently access their browser settings or follow complicated instructions and then alter privacy settings.

Websites discouraged users from opting out by stating that they will risk losing key services offered by the website. According to *Princess Isabella*, 'if you refuse to accept cookies you may be unable to make purchases or access certain parts of our Web Sites'. This means that readers are not really given the freedom to choose their privacy settings. Instead, they are forced to steer clear from opting out of cookies if they want to access the entire videogame service.

Privacy policies should inform children about the importance of adjusting their privacy settings otherwise they won't feel the need to opt out. Tracking mechanisms and methods to disable cookies should be easy to follow. It is recommended that *Clash of Clan's* policy should be followed, which has provided the simplest way to opt out by just clicking the 'opt-out' button next to the name of the third party.

The updated privacy policies have removed links that include complicated instructions on the methods to opt-out. Users are no longer expected to individually opt-out of several third-party interests and tracking mechanisms. Instead, they can choose to opt-out via email communication; choose not to accept cookies; unsubscribe links in any direct marketing email; or change the privacy settings on their device. Opt-out methods are now direct, and users can disable cookies right before playing a game or after registration through email communication. It is not clear that these methods are child-friendly. Advising children to alter their privacy settings by consulting browser documentation is a complicated process. Disabling

cookies resulting in the unavailability of the full list of services will deter users from opting out. Email correspondence creates its own set of difficulties. Emails can contain extensive information and it can be difficult to distinguish a malware email. In addition, it can be onerous for children to read emails and opt-out of cookies. They contain a lot of information and unless the method to disable cookies is a simple tick, it may be difficult to follow.

It is advised that websites should strive for a single tick to opt-out of cookies and similar tracking technologies for the benefit and ease in comprehension of children and their parents. *Clash of Clans* previously represented an easier method to opt-out by ticking three boxes. The updated privacy policy is more complicated in that clicking the opt-out button takes the user to the third-party privacy policy. The user is then expected to follow the method posted by the third party to disable tracking such as unsubscribing links through email communication. It is observed that although there is additional guidance for opting out, websites are still expecting users to consult browser documentation and/or read third party instructions for methods to opt-out. Children cannot be expected to read additional privacy policies. They should not be reading email correspondence from unidentified senders and clicking on their links without adequate supervision.

Table 15 analyses the tenth criterion, the parental consent mechanism.⁸⁶¹

5.5.10. Table 15 Criterion 10 – Parental consent mechanism

Criterion 10 – Parental consent mechanism
<p><i>Dota 2</i> – The website does not collect information from children under 13 years of age. Parents are encouraged to instruct their children about online privacy.</p> <p><i>Clash of Clans</i> – Personal information from children under 13 years will not be knowingly collected. If the website learns of any such possession, will delete the information immediately.</p> <p><i>Miniclip</i> – Children under 13 years can create a user account and participate in limited activities. The policy does mention that it will collect personal data to provide parental consent. However, it does not provide the kind of parental consent needed to authorise child participation</p> <p><i>Prince of Persia</i> – This is the only policy which clearly specifies the form of parental consent mechanism to authenticate a child’s participation. A child under 12 years will be required to provide the email address of a parent or guardian who will then be contacted to confirm the child’s participation. The policy even reserves the right to obtain written proof from the parent to obtain consent</p> <p><i>Heroes of the Storm</i> – The privacy policy does not mention anything about the minimum age for children or the parental consent mechanism</p> <p><i>League of Legends</i> – Children under 13 years are requested not to use the services or provide personal information. There is no form of parental consent mechanism</p> <p><i>Minecraft</i> – Use of the website by children under 13 years of age is blocked. The policy does mention the need for a parental consent and what happens once it is obtained; however it does not explain the form of parental consent that will apply</p> <p><i>Pogo</i> – Children under 13 years will not be allowed to input personal information, collect information for limited purposes and to obtain consent from parents for the collection, use and sharing of their children’s personal information. The policy does not mention the form of parental consent that will apply</p> <p><i>Candy Crush Saga</i> – The policy does not mention a parental consent mechanism and does not knowingly collect information from children under 13 years of age</p> <p><i>Princess Isabella</i> – The website does not knowingly collect information from children. Users under 16 years of age can only do so with the consent from a parent or responsible adult. There is no mention of the method of parental consent</p>

5.5.10.1. Failure to specify parental consent method

Apart from *Prince of Persia*, nine privacy policies failed to indicate a parental consent mechanism. This information can help parents to know what is required and in

⁸⁶¹ Children’s Online Privacy Protection Act of 1998 [15 U.S.C. §§ 6501–6506 \(Pub.L. 105–277, 112 Stat. 2681-728\)](#) enacted October 21, 1998) ; COPPA 16 C.F.R. § 312.5(c) COPPA requires requires website operators to obtain verifiable parental consent before collecting any personal information from a child under 13 years.

deciding if they prefer the particular method. The legal study relating to the methods of obtaining verifiable consent will be discussed in *Chapter 6*.

5.5.10.2. Unreliable methods for obtaining parental consent

Websites should acknowledge that the parental consent mechanism, like any identity authentication technology, can pose challenges. Websites requiring parental consent did not exhibit any standard format for ensuring that it was in fact the parent and not anyone else giving the consent. Research suggests that sending emails is considered the most proportionate and cost-effective form of obtaining a valid parental consent.⁸⁶² But children can find ways of providing false ages or fictitious emails to evade this formality. The industry should invest in innovate and more reliable forms of parental consent methods such as ‘face match to verified photo identification’ (FMVPI).⁸⁶³

Alternatively, owing to the difficulty associated with giving valid consent, website operators should rely on other ways to ensure children’s data remains safe and secure. Website operators should rely on data protection principles of minimality⁸⁶⁴ (see 3.2.3.3), transparency⁸⁶⁵ (see 3.2.4) and purpose specification⁸⁶⁶ (see 3.2.3.2) to ensure safety for children’s digital privacy⁸⁶⁷ (see 1.2.4; 4.10.3; 5.5.10.2).

⁸⁶² ‘Children’s Data Protection and Parental Consent’ (Advertising Education Forum, October 2013) <<http://www.aeforum.org/gallery/5248813.pdf>> accessed 31 January 2017.

⁸⁶³ ‘FTC Grants Approval for New COPPA Verifiable Parental Consent Method’ (Federal Trade Commission, 19 November 2015) <<https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>> accessed 19 March 2017.

⁸⁶⁴ Directive 95/46/EC Article 6(1)(c): The principle of minimality requires the collection of data to be adequate, relevant and not excessive; Directive 95/46/EC Recital 28; EU GDPR 2018 Article 5(1)(c).

⁸⁶⁵ EU GDPR 2018 Recital 58 and Article 5(1)(a).

⁸⁶⁶ Directive 95/46/EC Article 6(1)(b): Under the principle of ‘purpose specification’, data should be gathered for a specified, legitimate and compatible purpose; EU GDPR 2018 Article 5(1)(b).

⁸⁶⁷ ‘ICO GDPR Guidance’ (ICO, 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017.

None of the websites gave a consistent presentation of the responsibilities expected of parents when their children interact with the videogame. Parents were simply advised to supervise their children's online activities without realising that it would be impossible for parent's to permanently supervise them. This is inconsistent with research that suggests a limited number of parents can identify reliable, safe-to-access websites.⁸⁶⁸

The privacy policies updated in 2017/18 do not provide a parental consent method. However, they introduce the website's handling of children's data in a separate paragraph. The information is the same as before. Children under 13 should provide parental consent; and parents should advise children on the risks of sharing personal information online. An interesting observation was made in *Clash of Clans* which introduced a separate 'Parent's Guide'.⁸⁶⁹ This guide informs parents on payment transactions, in-app purchases, reporting on in-game problems and abuse. It also contains an 'online slang guide' which helps parents understand common terminology used by children when chatting with friends online.⁸⁷⁰ The document is helpful, but it should also advise parents to read privacy policies and discuss them with their children; to familiarise themselves with the working of cookies; inform them about the importance of altering privacy settings; and maintain up to date information with the website. Provision of an 'online slang guide' is an example of

⁸⁶⁸ Young Ji Lee, Sitwat Langrial and Wu-Chen Su, 'Are Parents Getting It Right? A Survey of Parents' Internet Use for Children's Health Care Information' (2015) 4(2) *Interact J Med Res*.

⁸⁶⁹ <http://supercell.com/en/parents/> accessed 18 May 2018.

⁸⁷⁰ *Ibid.* For example 'Noob' which means 'Someone who is new to the game or acts as though they are new to the game.'

good practice that treats children as a special class of data subjects and should be promoted in future data privacy laws.

Table 16 deals with the eleventh criterion, the rights of players with regards to subject access requests, which allow individuals to ensure that data held about them is accurate, whether it is being handled in accordance with data privacy rules and whether there is a need to correct and/or erase it.⁸⁷¹

⁸⁷¹ 'An Introduction to Subject Access Rights' (TaylorWessing, November 2013) <https://www.taylorwessing.com/globaldatahub/article_intro_sar.html accessed 20/03/2017> accessed 25 October 2016; 16 C.F.R. § 312.4(d)(3). Parents can request to review their children's data under COPPA.

5.5.11. Table 16 Criterion 11 – Players’ right to Subject Access Requests (SAR)

Criterion 11 – Players’ right to subject access requests
<p><i>Dota 2</i> – Users are granted access to view, correct or delete their information. The website may decline requests that are unreasonably repetitive, require disproportionate technical effort, jeopardise the privacy of others or are extremely impractical (under section heading ‘Corrections, Updates and Removal of Personally Identifiable Information’)</p>
<p><i>Clash of Clans</i> – Users are granted access to view, correct or delete their information (under section heading ‘Access to personal information’)</p>
<p><i>Miniclip</i> – Users are granted access to view, correct or delete their information (under section heading ‘Deleting, amending or updating your data’)</p>
<p><i>Prince of Persia</i> – Users are granted access to view, correct or delete their information (under Section 10 heading ‘How can you access and update your Personal Information and account profile?’)</p>
<p><i>Heroes of the Storm</i> – The policy does not mention providing users with the right to access, correct or delete their information (under section heading ‘What you should do if you wish to amend or review your personal information?’)</p>
<p><i>League of Legends</i> – Users are granted the right to access, update or delete their personal information (under Section 8 heading ‘Your choices and controls’)</p>
<p><i>Minecraft</i> – The policy provides detailed information concerning the editing and viewing of their personal information depending upon the Microsoft products they use (under section heading ‘How to access & control your personal data’)</p>
<p><i>Pogo</i> – The policy allows users to access and even deactivate their account. However, the website may request additional information to verify identity or request payment. The website can even reject requests that are unreasonable or impractical (under Section 8 heading ‘Your choices and controls’)</p>
<p><i>Candy Crush Saga</i> – The policy provides detailed information about the users right to access/view, correct, delete, account deactivation and direct marketing opt-out (under section heading ‘Your rights in relation to your information’)</p>
<p><i>Princess Isabella</i> – Users are granted access to view, correct or delete their information (under section heading ‘Accessing your information and your choices’)</p>

5.5.11.1. Discrepancy in the use of headings and subject access requests

Websites provided data subjects with the right to access/correct/delete their data. It was noticed that the headings for SARs were labelled differently. Pogo read ‘Your choices and controls’, *Princess Isabella* read ‘Accessing your information and choices’ and *Heroes of the Storm* read ‘What you should do if you wish to amend or review your personal information?’ Headings presenting the same right but worded

differently can cause confusion to children. It is advised that there should be a common heading for subject access requests which is self-explanatory.

Websites dealt differently with subject access requests. Some websites (*Miniclip*, *League of Legends* and *Dota 2*) provide a brief paragraph with an email address or an automated message box that can be used to send the request. Others (*Candy Crush Saga*, *Clash of Clans* and *Minecraft*) provide detailed information about the payment and time taken to process requests (*Princess Isabella*). Requests can be declined if they 'are unreasonably repetitive, require disproportionate technical effort, jeopardize the privacy of others, or are extremely impractical' (*Dota 2*). These are vaguely broad terms that can be used to decline requests for many reasons. For example, what is meant by 'disproportionate technical effort'? SAR policies should avoid declining requests based on broad, technically worded terms otherwise the purpose of the right is defeated.

5.6. Comparative privacy policy content analysis

The review featured 10 videogame websites selected based on popularity rankings and representing the legislation in the U.S., the EU and Canada.

The privacy policy was located on the main webpage, with no distinguishing features and a word length of up to 4,000 words. Following the update in the privacy policies in late 2017 and 2018 and some have increased the word length. Implied consent was previously assumed upon entering the website in all the privacy policies. The updated privacy policies have now removed the term 'implied consent'. Although four privacy policies are still using implying consent after the EU GDPR 2018 came into force on

25th May 2018. It is unclear if consent to the terms of the privacy policy is in the context of a written declaration, and the method in which this will be affected.

The privacy policy does not describe the purpose behind using privacy frameworks and independent seals. Children are expected to read lengthy, complicated documents and understand the purpose for themselves. The extensive collection of information raised concern for lack of specified purpose and even unambiguous consent. Tracking methods were worded in subtle ways and the method to opt out was difficult to follow.⁸⁷² Websites failed to mention the method of parental consent and data subjects' right to access was dealt with in separate ways.

Children will find it hard to read lengthy, complicated documents and struggle to recognise the importance of altering their privacy settings. They should be facilitated with information that is easy to understand rather than burden them with reading copious amounts of information that will certainly be debilitating.

The previous sections detailed the findings of the multiple case study by analysing the criteria to evaluate privacy policies. The next section will put forth detailed findings from the study of the stages of subscription if any.

5.7. The registration procedure in videogame websites

Investigation of the registration procedure is important because it is the first point of consent between the user and the website. Children will be required to register and become a member before they can start to play the game. It is imperative for websites to take account of children's ease in divulging personal information

⁸⁷² David Wright and Reinhard Kreissl, *Surveillance in Europe* (Routledge 2015) 294.

belonging to them and third parties (parents/legal guardians). Do websites cater to the needs of children? Does it explain the reason for requesting their personal information?? Can children play the game without registration?

5.7.1. Key findings regarding the study of registration procedures for videogame websites

From the analysis of the privacy policies, the next stage was to sign up to the terms of the policies and three distinct forms of registration procedures were noted. Firstly, the player can continue playing a game advertised as 'free to play' but eventually required to register to access additional services. In *Candy Crush Saga* and *Miniclip*, the player could play the game without the requirement of registering or creating an account but, after clearing a few levels, could only progress further after having registered as a member.

In the second form of registration procedure, the game could be played without registering, as in *Pogo*, but there were still persistent messages to register. The phrase 'Why Register' was hyperlinked and opened into another document, stating that players can access over 1,000 games, win prizes and earn tokens to spend on virtual items if they registered onto the website.

In the third form of registration, the game was advertised as 'free to play now', as in *Heroes of the Storm*, *Dota 2* and *League of Legends*. In *Dota 2*, the game required the player to download the program 'Steam' before they could progress any further. Once the download was complete, it was followed by a message box wanting permission 'to allow the program to make changes to the computer'. The program

did not specify what these changes were. To proceed further, consent had to be given, which started to install an unfamiliar program. Once this installation was complete, the player was redirected to the login page and had to create an account.

Even though some games were worded as 'play now' and 'play for free now', players were still expected to register by giving away some components of their personal information. Others were downloading and installing programs while providing uninformed consent. Most of the games required the player to depart with some form of personally identifiable information such as email address, date of birth and gender, which featured most commonly. Pogo asked the player to provide the country of their residence. In Pogo, there was a question mark button placed in front of the email address and date of birth to explain why this information was collected. These were short pieces of information and very useful to gain a quick understanding behind collecting information. This practice was not observed in the rest of the games.

5.8. Conclusion and recommendations regarding privacy policies for children

The policies were shorter and easier to read following an update on 1 January 2017. The recent EU GDPR 2018 may have influenced the update leading to an increased word count for most privacy policies. For the first time, EU law recognised that children may be less risk averse online and need special digital protection (*see 3.2.4*).⁸⁷³ Privacy notices should be transparent, clear and in plain language so that

⁸⁷³ EU GDPR 2018 Recital 38.

the message can resonate with children and they can understand the message that is directed.⁸⁷⁴

It was found that in the updated privacy policies, the term 'Privacy Policy' is placed at the bottom of the page without any distinguishing features. Only the updated privacy policies have removed complicated terms such as 'web beacons' whereas the rest are still using such terms. Although complicated privacy frameworks such as the TRUSTe Privacy Certification is still being used.

One of the major concerns encountered was the sheer volume of personal information collected from children. Legally, websites should have a purpose before they can collect personal data. The word 'purpose' has been defined broadly by the law, thus allowing the website operator to collect information without clearly explaining what the 'purpose' is. Policies should provide an exhaustive list, giving clear and specific reasons to improve transparency and legitimacy of data collection. The opt-out mechanism is still a complicated process even after the recent update. Children have to consult their browser documentation or click on third party websites with their own instructions for methods to opt-out. Policies should explain to children about the privacy risks associated with tracking technologies and the need to alter their privacy settings.

⁸⁷⁴ EU GDPR 2018 Recital 58; Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa 11 April 2018) [file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018.

The 'online slang guide' for parents contained in Clash of Clans is helpful information. Such practices should be encouraged as they aim to treat children as a special class of data subjects.

Apart from *Prince of Persia*, the policies failed to describe the method for obtaining parental consent. It may not be required by the law, but the multiple case study revealed that it is good practice to keep parents informed about the consent mechanisms. The updated privacy policies do deal with the websites handling of children's data in a separate paragraph, but the information remains the same. The website operator must take notice of the large number of younger audience members the website attracts and formulate a brief, easy-to-read and simple privacy policy. Websites should strive to introduce a separate brief, simple and child-friendly privacy policy for children and their parents.

This study has concluded the multiple case study analysis in respect of the privacy policies and registration procedure for each game. The next chapter will carry out the second part of the multiple case study, which will examine if privacy policies are compatible with governing data privacy laws. This is a significant study as it will correlate industrial practice with the legal requirements. It will explore whether the findings from this chapter remain compatible with jurisdiction-based data privacy laws. Such a critical analysis will illuminate any differences between law and practice. The comprehensive scrutiny can lay down foundations for proposals to fill up any gaps between the law and actual practice. The study will also involve a detailed analysis of how the law and industrial practice affect children as regular users of the videogames websites who are expected to read, understand and consent to the

terms of the privacy policies. Therefore, even if the privacy policies adhere to governing law, the system should be sufficiently attentive and accommodating to the needs of children who are avid users of videogames.

CHAPTER SIX

PART 2 – ONLINE GAMES CASE STUDIES: PRIVACY POLICIES AND GOVERNING DATA PRIVACY LAW

6.1. Introduction

Chapter 5 carried out the first part of the multiple case study. It analysed whether the privacy policies of 10 popular videogames comply with the expectation that children should read, understand and consent to their terms. It concluded that videogame privacy policies are lengthy documents, use technical and legal jargon and collect extensive information from users without clearly explaining the purposes for doing so, consent is difficult to prove, and parental consent mechanism is unclearly illustrated in the privacy policies. The videogames fail to provide the specific law that governs the data handling practices and users will be unaware of the rights and obligations they are entitled to.

Chapter 6 carries out the second part of the multiple case study to evaluate the compatibility of privacy policies with governing data privacy law, beginning in the U.S. and followed by the EU. Section 6.2 critically analyses the criteria for evaluating privacy policies (*Chapter 5 Table 4*) studying the U.S.-based data protection and privacy laws that regulate them. Section 6.4 carries out a similar analysis undertaken in Section 6.2 while considering EU data privacy laws.

6.2. Overview of the key legislation in the U.S. and EU for evaluating privacy policies

The games have been colour-coded to highlight the legislatures they represent (*Chapter 5 Table 5*) Games governed by European data privacy laws⁸⁷⁵ will be considered with respect to provisions of the earlier Directive 95/46/EC⁸⁷⁶ and the EU GDPR 2018 which is in force since 25th May 2018.⁸⁷⁷ Games governed by U.S. data privacy laws⁸⁷⁸ will be evaluated using the Children’s Online Privacy Protection Act 1998 (‘COPPA’),⁸⁷⁹ the California Online Privacy Protection Act 2003 (‘CalOPPA’),⁸⁸⁰ the Delaware Online Privacy Protection Act (‘DOPPA’)⁸⁸¹ and Washington State’s data privacy laws. Some games are governed by both U.S. and EU data privacy laws⁸⁸² but they will be considered separately under both legislatures to avoid duplicity. The list (*Chapter 5 Table 5*) lacks a game governed by the Canadian data privacy law, PIPEDA (*see 5.3.1.3*). The multiple case study of videogames regulated by U.S. data privacy policies will be studied first.

⁸⁷⁵ Miniclip, *Prince of Persia*, *Heroes of the Storm* and *League of Legends*.

⁸⁷⁶ European Parliament and Council Directive [95/46/EC](#) of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ; European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (Council of Europe, 4 November 1950) <<http://www.refworld.org/docid/3ae6b3b04.html>> accessed 24 March 2016.

⁸⁷⁷ ‘The History of the General Data Protection Regulation’ (Europa) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 11 December 2017.

⁸⁷⁸ *Clash of Clans*, *Dota 2*, *Princess Isabella*, *Candy Crush Saga*, *Minecraft* and *Pogo*.

⁸⁷⁹ Milda Macenaite and Eleni Kosta, ‘Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps’ (2017) 26(2) *Information & Communications Technology Law* 146.

⁸⁸⁰ California Online Privacy Protection Act 2003– California Business and Professions Code Sections 22575–22579.

⁸⁸¹ Title 6 Commerce and Trade Subtitle II Other Laws Relating to Commerce and Trade Chapter 12c. Online and Personal Privacy Protection.

⁸⁸² *Minecraft*, *Pogo*, *Candy Crush Saga* and *Clash of Clans*.

- Games governed by United States law
- Games governed by European law
- Games governed by Canadian Law

Table 17 evaluates the first criterion, namely the ‘location of privacy policy’ of videogames governed by U.S. data privacy laws (*Chapter 5 Table 4*).

6.2.1. Table 17 Criterion 1 – Location of privacy policy

Criterion 1 – Location of privacy policy
Washington State privacy laws – There are no rules on the location of privacy policy
CalOPPA – Privacy policy to be posted on the homepage or first significant page after entering the website, ⁸⁸³ with certain distinguishing features ⁸⁸⁴
DOPPA – The provisions for location of privacy policy are similar to CalOPPA ⁸⁸⁵
COPPA – The website should post a notice a clearly labelled and prominent link to an online notice collecting information ⁸⁸⁶

In nine out of 10 videogames, the privacy policy is located at the bottom of the main webpage and does not exhibit any striking features (different colour, font or size)⁸⁸⁷ (*see 4.4 and 4.4.1*). The FTC does not consider ‘clear and prominent’ a link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other adjacent links,⁸⁸⁸ unless it is presented in a clear and prominent

⁸⁸³ CalOPPA 22577(b)(1).

⁸⁸⁴ CalOPPA 22577(b)(2).

⁸⁸⁵ DOPPA § 1202C(7).

⁸⁸⁶ 16 CFR Section 312.4(d).

⁸⁸⁷ The privacy policies were not compatible with the legal requirement to highlight privacy notices. CalOPPA and DOPPA require clear labelling, prominent placement and distinguishing features but there is no guidance on the exact location of the privacy policy, as long as it is contained on the main webpage.

⁸⁸⁸ Federal Trade Commission, ‘Children’s Online Privacy Protection Rule’ (1999) 64 Federal Register 212.

manner.⁸⁸⁹ The law requires prominence and contrasting features for privacy policies but, in practice, neither was displayed.

It will be easier for children to locate the privacy policy if it is placed at the top of the homepage and exhibiting distinguishing features such as a large font, size or different colour. The law should avoid using terms that are susceptible to broad interpretations. For example, DOPPA states that the policy should be visible to a reasonable person.⁸⁹⁰ Who is defined as a reasonable person? COPPA requires the policy to be clearly labelled without specifying the meaning of 'clearly labelled'. Does it have to be the most prominent word or one of the most prominent words on the homepage? Therefore, words that can create confusion should be avoided.

Table 18 considers the second criterion, the length and wording of the privacy policy.

6.2.2. Table 18 Criterion 2 – Length and wording of the privacy policy

Criterion 2 – Length and wording of the privacy policy
Washington State privacy laws – There are no rules on the length and wording of the privacy policy
CalOPPA – CalOPPA does not have any legal requirements regarding the length and wording including readability of the privacy policy. However, California’s attorney general has provided a guide regarding readability, ⁸⁹¹ which will be discussed in the analysis below
DOPPA – There are no provisions that deal with the wording or readability of the policy
COPPA – There are no provisions in COPPA on the length of the document. With reference to the readability of the policy, COPPA requires that the operator of a website, in giving notice to parents regarding their children’s data collection, must be clearly and understandably written, be complete and not contain confusing or contradictory materials ⁸⁹²

⁸⁸⁹ 'Complying with COPPA: Frequently Asked Questions' (Federal Trade Commission) <<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>> accessed 9 March 2017.

⁸⁹⁰ DOPPA § 1202C(d).

⁸⁹¹ 'Making Your Privacy Practices Public' (California Department of Justice, May 2014) <https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf> accessed 6 March 2017.

⁸⁹² 16 CFR Section 312.4(a).

The privacy policies presented an average word length of 4,000 words. California's Attorney General advises that privacy policies be concise, plain and simple.⁸⁹³ It does not explain how plain the English should be, or the appropriate length of the document intended for children to read. Privacy policies should employ the Flesch reading test⁸⁹⁴ with a reading score of 100–90, or 'very easy to read', which is suitable for a grade 5 or 11-year-old child (see 5.5.2.2 and 5.5.2.3; 8.6.1).

In other industries, newspapers have realised that easy reading will promote learning and enjoyment.⁸⁹⁵ *Reader's Digest* and *TV Guide* are the publications with the largest circulations and are written at the ninth-grade level.⁸⁹⁶ Comics have a Flesch reading score of 92, which means that they can easily be read by a fifth-grade or 11-year-old child; *Time* magazine is scored at 52 and is aimed at students in twelfth grade.⁸⁹⁷ The Law Society has also backed the Plain English Campaign and encouraged legal professionals to remove Latin jargon and make legal documents easily accessible and legible to clients.⁸⁹⁸ There is a wide understanding that children should learn and enjoy reading literature. But they are required to read lengthy, complicated privacy policies.

⁸⁹³ 'Making Your Privacy Practices Public' (California Department of Justice May 2014) <https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf> accessed 6 March 2017.

⁸⁹⁴ 'Flesch Reading Ease Readability Formula' (Readability Formulas) <<http://www.readabilityformulas.com/flesch-reading-ease-readability-formula.php>> accessed 6 March 2017.

⁸⁹⁵ Edward Fry, 'Readability' Reading Hall of Fame Book' (International Reading Assn, 2006) <<http://www.impact-information.com/impactinfo/fryreadability.pdf>> accessed 26 January 2018.

⁸⁹⁶ William H. Dubay, 'Smart Language: Readers, Readability, and the Grading of Text' (Impact Information, 2007) <<http://www.impact-information.com/impactinfo/newsletter/smartlanguage02.pdf>> accessed 26 January 2018.

⁸⁹⁷ Grant Draper, 'Writing and Readability Scores: It Matters' (Marketingprofs, 3 January 2014) <<http://www.marketingprofs.com/articles/2014/12377/writing-and-readability-scores-it-matters>> accessed 26 January 2018.

⁸⁹⁸ 'Language Barrier' *The Law Society Gazette* (10 June 2004) <<https://www.lawgazette.co.uk/news/language-barrier/42217.article>> accessed 26 January 2018.

6.2.3. Table 19 Criterion 3 – Governing legislation

Criterion 3 – Governing legislation	
Washington State data privacy laws	<i>Minecraft, Dota 2 and Princess Isabella</i> are governed by the laws of the state of Washington, USA
CalOPPA	<i>Clash of Clans</i> and Pogo are governed by the laws of California – <i>Clash of Clans</i> is governed by the laws of California and Finland
DOPPA	<i>Candy Crush Saga</i> is governed by the laws of the state of Delaware

6.2.3.1. Absence of a specifically applicable law

A legal issue has been identified in the study that none of the videogames provides a specifically applicable legislation (see 5.4.1; 6.6.2; 8.6.2). Two issues arise from this. Firstly, users need to know about their rights and obligations under the data privacy law. Different countries apply different levels of protection and the governing law should be set out from the beginning. This is the case with videogames governed by both EU and U.S. data privacy laws,⁸⁹⁹ which are very different in nature (see 4.7 and 4.11). Secondly, users from non-legal backgrounds will be carrying out independent research, undertake complicated legal expeditions and make speculations about the possible law that governs the terms of the privacy policy.

It is customary practice that governing law is embedded within the contractual terms and refer widely to the laws of the land such as ‘laws of England’. Further, it can be argued children may not have the necessary legal expertise to understand the rights and obligations arising out of statutes. It is asserted that, since children are expected to consent to privacy policies and submit some part of their personal information,

⁸⁹⁹ Chapter 5 Table 5 colour coded blue, representing *Clash of Clans, Minecraft, Pogo* and *Candy Crush Saga*.

take part in surveys, participate in chat rooms and make contributions towards forums in the videogame, they should be able to understand what they are consenting to. Additionally, they should also be able to understand key provisions of the law. They should comprehend any rights and obligations they are entitled to under the data privacy law governing the data gathering practices of the privacy policy (see 5.4.1 & 5.5.2.4).

It is recommended that in addition to contractual laws contained in the terms of service, the privacy policy should provide a link to a reputable source of data privacy law. For instance, the videogame Miniclip is governed by 'laws of England' (*Chapter 5 Table 5*). This thesis recommends that Miniclip privacy policy should specify it is governed by the EU GDPR 2018 and Data Protection Act 2018 (see 1.1.1 & 1.1.2). The privacy policy should contain a link a reputable source such as the Information Commissioner's Office in the UK that presents the data privacy law and updates it accordingly.

6.2.3.2. Varying levels of data protection in the U.S.

Data users should be aware of the law that applies to them so that they can make informed decisions about submitting personal information. The differing ages for consent mean that children will not be given special protection uniformly. In videogames, there are various parties involved in the international context, allowing the contract to be connected to several places.⁹⁰⁰

⁹⁰⁰ "Governing law" and "jurisdiction" clauses (Lexology)
<<http://www.lexology.com/library/detail.aspx?g=469b7d6f-4f8c-44cb-9f10-dcdd1edf20bf>> accessed 6 March 2017.

6.2.3.3. Washington State does not have a specific data privacy law

It was difficult to determine the data privacy law for Washington (*see 4.6*). *Dota 2* had a 'jurisdiction clause' that gave exclusive jurisdiction to federal and state courts located at King County, Washington, to preside over any claim arising out of the agreement.

Washington State has a myriad of statutes that tackle an individual's right to privacy,⁹⁰¹ with little information on how it applies to data privacy practices. Independent study is required to investigate the matter, with unclear results. It will be significantly difficult for a child or a person of non-legal background to retrieve the law that applies to them.

The term 'without reference to its choice of law rules' mean that Washington State laws will apply even if the cause of action occurred in California. It is not clear if CalOPPA will remain relevant owing to its wide-ranging application. Will the Washington State laws take precedence if the cause of action occurs in California?

Ken Adams, an expert and author on contract drafting⁹⁰² has considered in detail the governing law provisions. He is of the view that courts can just consider the substantive law of the jurisdiction right away, instead of using choice of law principles as a basis for deciding to apply a different law.⁹⁰³ He found that even if a choice of law is made, nothing can stop the courts of a U.S. jurisdiction to decide otherwise or

⁹⁰¹ 'Privacy Modelling Tool' (watech) <https://watech-beta.herokuapp.com/user_guide> accessed 6 March 2017. Washington State's constitutional right to privacy encapsulated an individual's right to their personal information in Article 1 Section 7, which prohibits the invasion of private affairs or homes of individuals.

⁹⁰² Ken Adams, 'A Manual of Style for Contract Drafting' (American Bar Association, 2013) and 'The Structure of M&A Contracts' (LegalWorks, 2016).

⁹⁰³ Ken Adams, 'Simplifying Governing-Law Provisions, Part 2' (Adams, 13 July 2015) <<http://www.adamsdrafting.com/simplifying-governing-law-provisions-part-2-renvoi/>> accessed 7 March 2017.

indulge in any ‘choice of law shenanigans’.⁹⁰⁴ He questions the aim of parties who contract, for example, that ‘New York law shall govern’. Do they intend that New York substantive law or local law will prevail or the whole of New York shall govern?.⁹⁰⁵ He agrees that, if the choice of law is not valid, courts will not apply it. This means that if the cause of action occurred in California, CalOPPA may still be applicable, even if the policy says otherwise.

Table 20 analyses the fourth criterion, ‘Privacy Shield Framework to safeguard transfer of data between the EU and the U.S’ (see 5.5.4).

6.2.4. Table 20 Criterion 4 – Privacy rules involving Privacy Shield Framework to safeguard transfer of data between the EU and the U.S.

Criterion 4 – Privacy rules involving the Privacy Shield Framework to safeguard transfer of data between the EU and the U.S.	
Washington State privacy laws	A link between Washington State privacy laws and the Privacy Shield Framework could not be established
COPPA	COPPA does not give any provisions on the EU–U.S. Privacy Shield Framework
CalOPPA	CalOPPA does not have any provisions on the EU–U.S. Privacy Shield Framework
FTC	The FTC facilitates the EU–U.S. Privacy Shield Framework ⁹⁰⁶

There are 23 Privacy Shield Principles⁹⁰⁷ that impose stronger obligations on U.S. companies, involving an annual self-certification that they meet data privacy rules.⁹⁰⁸

⁹⁰⁴ Ken Adams, ‘Simplifying Governing-Law Provisions, Part 2’ (Adams, 13 July 2015) <<http://www.adamsdrafting.com/simplifying-governing-law-provisions-part-2-renvoi/>> accessed 7 March 2017.

⁹⁰⁵ Ibid.

⁹⁰⁶ Edith Ramirez, ‘ANNEX IV’ (Europa, 23 February 2016) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-4_en.pdf> accessed 28 March 2017.

⁹⁰⁷ ‘Requirements of Participation’ (Privacy Shield Framework) <<https://www.privacyshield.gov/article?id=Requirements-of-Participation>> accessed 28 March 2017.

⁹⁰⁸ European Commission, ‘EU-U.S. Privacy Shield’ (Europa July 2016) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf> accessed 14 March 2017. The website should display a privacy policy on their website, reply promptly to complaints, and cooperate with the European data protection authorities when handling human resources.

It has already been established in *Chapter 5 Section 5.5.4* that the eligibility criteria for the privacy framework is unclear and the link opens onto lengthy, complicated and legal documents.⁹⁰⁹ Such frameworks should be avoided in children’s privacy policy as they have commercial significance only.

In the next section, the fifth criterion, ‘TRUSTe privacy certification’, is discussed with regards to the legislation that authenticates it (*see 5.5.5*).

6.2.5. Table 21 Criterion 5 – TRUSTe privacy certification

Criterion 5 – TRUSTe privacy certification	
Washington State privacy laws	There are no provisions on TRUSTe privacy certification
COPPA	TRUSTe has collaborated with the FTC-enforced COPPA to deliver COPPA Safe Harbour certifications for children’s privacy programme ⁹¹⁰
CalOPPA	TRUSTe privacy assessment and certifications collaborate with CalOPPA

TRUSTe is applied by *Clash of Clans* and Pogo as a link that can be clicked to access additional information, which can be up to 26 pages long.

⁹⁰⁹ EU-U.S. Privacy Shield Framework principles issued by the U.S. Department of Commerce (Europa) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf> accessed 28 March 2017.

⁹¹⁰ ‘Kid’s Privacy/COPPA Assessments & Certifications’ (TRUSTe) <<https://www.trustarc.com/products/coppa-certification/>> accessed 7 March 2017.

TRUSTe has come under criticism in recent years (*see* 5.5.5). The FTC agrees that consumers cannot themselves evaluate the privacy practices of websites and rely on third-party seals trusted for their expertise and independence.⁹¹¹

If TRUSTe guarantees a standard of privacy, it is not clear what this standard is. For example, paragraph II(A)(1) of the TRUSTe Children's Privacy Certification Standard provides that businesses complying with TRUSTe should demonstrate a privacy notice that is approved by TRUSTe.⁹¹² What standard should be met by the privacy notice to be approved by TRUSTe?

There is a lot of information that the user may have to go through to understand the level of privacy that is accorded to them. Otherwise, it is just a logo with no meaning. The programme may have little value for children and should preferably not be used in privacy policies directed to them.

⁹¹¹ 'TRUSTe Settles FTC Charges It Deceived Consumers through Its Privacy Seal Program' (Federal Trade Commission, 17 November 2014)

<<https://webcache.googleusercontent.com/search?q=cache:ukbYgSaiy4sJ:https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 28 March 2017. The FTC brought a complaint against TRUSTe for failure to conduct annual recertifications of companies holding TRUSTe privacy seals. In addition, the FTC's complaint alleged that, since TRUSTe became a for-profit corporation in 2008, the company had failed to require companies using TRUSTe seals to update references to the organisation's non-profit status. Easwar A. Nyshadham, 'Privacy Policies of Air Travel Websites: A Survey and Analysis' (2000) 6(3) *Journal of Air Transport Management* 143. Easwar A. Nyshadham carried out a study of the privacy policies of 23 airlines to determine if they complied with fair information practices. It was found that very few firms complied with the principles even though some of them had received seals of approval from TRUSTe.

⁹¹² <<https://www.trustarc.com/privacy-certification-standards/>> accessed 28 March 2017 This information is contained on the TRUSTe homepage certification standards table titled 'Children's Privacy Certification Standard'.

Table 22 presents the sixth criterion, the ‘collection of personal information’.

6.2.6. Table 22 Criterion 6 – Collection of information from children

Criterion 6 – Collection of information from children	
Washington State privacy laws	There are no rules for the collection of personal data
CalOPPA	CalOPPA defines ‘personally identifiable information’ as identifying an individual and provides a list of elements such as first and last name, telephone number, information that can be passively collected by the site such as geo-location data, device identifier etc. ⁹¹³ The operator will have to define the categories of information to be collected by the website ⁹¹⁴
DOPPA	DOPPA mirrors the definition of ‘personally identifiable information’ ⁹¹⁵ as contained in CalOPPA ⁹¹⁶
COPPA	Termed ‘personal information’, COPPA mirrors the definition of ‘personally identifiable information’ ⁹¹⁷ as contained in CalOPPA and DOPPA. An operator of a website directed to children will have to notify what information is collected; how it is used; and the disclosure practices of such information if the operator has knowledge that it is collecting information from children ⁹¹⁸

Websites tended to collect extensive information from users without giving exact reasons behind the collection (see 5.5.6; 6.6.4; 8.6.3). Websites would typically use vague terms such as ‘to improve products or services’ as a legitimate reason for collecting data (see 3.2.3.2). This position has altered with the updated privacy policies which avoid using such purposes to justify collection of personal information.

⁹¹³ CalOPPA 22577 (a).

⁹¹⁴ CalOPPA 22575(b)(1).

⁹¹⁵ DOPPA § 1202C(15).

⁹¹⁶ DOPPA § 1205C(b)(1).

⁹¹⁷ COPPA § 6501(8).

⁹¹⁸ COPPA § 6502(b)(1)(A)(i).

6.2.6.1. Extensive information collected from users

The Attorney General of California⁹¹⁹ has advised websites collecting personal information⁹²⁰ to remain specific and concise, with a minimum list of the categories of information collected from visitors.⁹²¹ COPPA also prevents websites from conditioning a child into disclosing more personal information than is reasonably necessary to participate in the activity.⁹²² Even though law should define the terms ‘minimum’ and ‘reasonably necessary’, legal guidance should also mention the quantity of personal information reasonably necessary from children.

Table 23 deals with the seventh criterion, namely third parties collecting personal information.

6.2.7. Table 23 Criterion 7 – Third parties collecting personal Information

Criterion 7 – Third parties collecting personal Information
Washington State privacy laws – There are no rules that govern the practice of third parties collecting personal information from the host website
COPPA – COPPA requires website operators to post a prominent notice or a clearly labelled link to a notice on the homepage and at each area of the website where personal information is collected from children. ⁹²³ Such a notice should also list the names, addresses, telephone numbers and email addresses of all the operators that are collecting or maintaining personal information from children ⁹²⁴
CalOPPA – According to CalOPPA, website operators have to identify the categories of third parties with whom the operator may share that personal information ⁹²⁵
DOPPA – DOPPA expects website operators to disclose the categories of third parties that may collect personal information about a user’s online activities ⁹²⁶

⁹¹⁹ ‘Making Your Privacy Practices Public’ (California Department of Justice, May 2014)
<https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf>
accessed 7 March 2017.

⁹²⁰ Ibid.

⁹²¹ California Business and Professions Code § 22575(b)(1).

⁹²² COPPA 16 CFR 312.7.

⁹²³ COPPA 16 CFR 312.4 (d).

⁹²⁴ COPPA 16 CFR 312.4 (d)(1).

⁹²⁵ CalOPPA 22575(b)(1).

⁹²⁶ DOPPA § 1205C(b)(c).

Data privacy laws fall short of the need for explaining to children the term ‘third parties’ and their purpose for collecting information. Website operators are only obliged to indicate ‘the categories of data’ collected by third parties without explaining the term ‘category’.

Laws should require websites to identify third parties, state that they are operating on the website, and provide information about the data they collect and why. These rules should not apply to children’s privacy policies, which will make the document lengthy and complicated. Additionally, operators need to rethink the number of third parties operating on their website and maintain a balance between the digital privacy rights of children and the need for third parties to collect their information.

Table 24 will deal with the eighth and ninth criteria, namely cookies and third-party tracking technology and disabling cookies and third-party technology. Since the disclosure of cookies and tracking technologies as well as the methods to disable them is regarded simultaneously in legislative provisions, it would be convenient to consider the two criteria under the same heading.

6.2.8. Table 24 Criterion 8 – Cookies and third-party tracking technologies – and Criterion 9 – Methods to disable cookies and other third-party tracking technologies

Criterion 8 – Cookies and third-party tracking technologies – and Criterion 9 – Methods to disable cookies and other third-party tracking technologies
<p>CalOPPA – In 2013, the California Legislature passed AB 370, a ‘tracking transparency’ law that amends CalOPPA by adding disclosures about online tracking to the requirements for a privacy policy⁹²⁷</p> <p>COPPA – COPPA prevents a website or online service from collecting personal information from children under the age of 13, without a verifiable parental consent.⁹²⁸ In December 2012, the FTC updated the COPPA rule to expand the definition of ‘personal data’ to include persistent identifiers.⁹²⁹ Operators should provide notice to parents to obtain verifiable parental consent before collecting, using or disclosing the information⁹³⁰</p> <p>FTC – The FTC has provided guidance to consumers on variant methods of tracking, how they work, and how users can control such tracking⁹³¹</p> <p>DOPPA – DOPPA requires website operators to respond to web browser ‘do not track’ signals that provide users the ability to exercise choice regarding the collection of personally identifiable information about the user’s online activities which allow users to disable tracking mechanisms.⁹³² There is no clear provision that mentions cookies and third-party tracking technologies</p>

⁹²⁷ Dominique Shelton, ‘California Adopts Do-Not-Track Disclosure Law: A.B. 370 Amends the California Online Privacy Protection Act (CalOPPA) to Require New Privacy Policy Disclosures for Websites, Online Services and Mobile Apps about Behavioral Tracking’ <<http://www.alstonprivacy.com/california-adopts-do-not-track-disclosure-law-a-b-370-amends-the-california-online-privacy-protection-act-caloppa-to-require-new-privacy-policy-disclosures-for-websites-online-services-and-mobile/>> accessed 7 March 2017; Consumers: Online Tracking: Hearing on AB 370 (Muratsuchi) Before S. Comm. on the Judiciary, 2013- 2014 Reg. Sess. (June, 18, 2013) <[leginfo.legislature.ca.gov](http://leginfo.ca.gov)> accessed 29 March 2017. AB 370 will allow consumers to learn from a website’s privacy policy whether or not that website honours a do not track signal. This will allow the consumer to make an informed decision about their use of the website or service.

⁹²⁸ COPPA 15 U.S. Code § 6501(1) and 6502(b)(ii).

⁹²⁹ ‘Revised Children’s Online Privacy Protection Rule Goes into Effect Today’ (Federal Trade Commission, 1 July 2013) <<https://webcache.googleusercontent.com/search?q=cache:iwahN-q3VZoj:https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect+%cd=3&hl=en&ct=clnk&gl=uk>> accessed 30 March 2017; 16 CFR 312.2 Persistent identifiers can include identifiers, such as a customer number held in a cookie, an IP address, a processor or device serial number, or a unique device identifier that can be used to recognise a user over time and across different websites or online services.

⁹³⁰ COPPA 15 U.S. Code § 6502.

⁹³¹ Consumer information (Federal Trade Commission) <<https://www.consumer.ftc.gov/articles/0042-online-tracking>> accessed 29 March 2017; Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers, Preliminary Staff Report (Federal Trade Commission 2010) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>> accessed 7 March 2017; ‘What Is Do Not Track’ (Future of Privacy Forum) <<https://webcache.googleusercontent.com/search?q=cache:iR4bdoTXI9J:https://allaboutdnt.com/+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 7 March 2017; California Business and Professions Code Section 22575(b)(5); California Business and Professions Code Section 22575(b)(6). The FTC proposed a do not track (DNT) browser signal, which empowers consumers to choose whether to allow the collection and use of their personal information regarding their online activities. Currently there is no universal standard or legal requirement for how operators of web sites or online services must respond to a browser’s DNT signal. The new law requires two new disclosures in the privacy policy of a web site subject to CalOPPA in the form of the operator’s response to a browser DNT signal or to ‘other mechanisms’ and the possible presence of other parties conducting online tracking on the operator’s site or service.

⁹³² DOPPA § 1205C(b)(5).

Websites employ various tracking methods without explaining them. Legal guidance fails to provide the extent of tracking technologies that can be used or the need to caution websites against the use of flash cookies, which is a more intrusive form of tracking method (see 3.3; 5.5.8.1; 6.4.6; 8.6.4).⁹³³

The FTC takes notice of the management and new forms of tracking mechanisms. The FTC complained against Nomi Technologies for failing to provide consumers with an opt-out mechanism after undertaking in its privacy policy that it will do so.⁹³⁴ Recently, it brought a complaint against a new form of tracking called cross-device tracking tools that tracks by linking activity across devices.⁹³⁵ FTC also complained against Vizio for tracking television viewers and then selling their viewing histories to advertisers and others.⁹³⁶

The FTC is actively shaping the U.S.'s data tracking scene, but any guidance provided in this regard is not sufficiently tailored to the needs of children who frequently visit videogame websites. In the above cases, FTC's involvement is based on misleading or no information about the companies' tracking mechanisms. If the tracking methods are not explained clearly, or too many are employed, children will fail to recognise their purpose, and this should also be a point of concern for the FTC.

⁹³³ There are various privacy risks associated with the use of flash cookies.

⁹³⁴ Retail tracking firm settles FTC charges it misled consumers about opt out choices (Federal Trade Commission 23 April 2015) <<https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers>> accessed 30 March 2017.

⁹³⁵ Cross-device tracking (Federal Trade Commission January 2017) <https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf> accessed 30 March 2017.

⁹³⁶ Lesley Fair, 'What Vizio was doing behind the TV screen' (Federal Trade Commission 6 February 2017) <<https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen>> accessed 30 March 2017.

6.2.8.1. Methods to disable/opt out of tracking were not easy to follow

Methods to disable/opt out of cookies and tracking mechanisms were complicated and difficult to follow. Legislation should preferably require website operators to use simple language and explain tracking methods, their purpose, and the extent of use, which can be proportionately balanced against the age and best interests⁹³⁷ of the data subject. The privacy policies updated in 2018 attempted to define the opt-out methods. However, users are still expected to either consult their browser documentation, unsubscribe links in email correspondence or visit the third-party website privacy policies and follow their instructions on opting out (see 5.5.9.1).

⁹³⁷ UNCRC Article 3. Adults should think about the best interests of children and young people when making choices that affect them.

Table 25 considers the tenth criterion, namely the parental consent mechanism.

6.2.9. Table 25 Criterion 10 – Parental consent mechanism⁹³⁸

Criterion 10 – Parental consent mechanism	
Washington State privacy laws	There are no rules on a parental consent mechanism
COPPA	Website operators have to obtain verifiable parental consent from parents before collecting any personal information from children under 13 years of age ⁹³⁹
CalOPPA	The attorney general states that websites collecting personal information from children under 13 years of age will apply the requirements of COPPA including obtaining verifiable parental consent prior to collecting information from children ⁹⁴⁰
DOPPA	DOPPA does not provide a parental consent mechanism but focuses on additional substantive elements of how data about children (under 18-year olds) can be used ⁹⁴¹ and places prohibitions on online marketing or advertising to a child ⁹⁴²
FTC	The FTC promotes several non-exhaustive lists of obtaining parental consent and the FTC can be applied for pre-approval of a new form of consent mechanism ⁹⁴³

COPPA is open to the use of any number of methods to obtain verifiable parental consent, as long as the method is reasonably calculated,⁹⁴⁴ in light of available technology to ensure that the person providing consent is the child’s parent.⁹⁴⁵ The term ‘reasonably calculated’ is very vague and some of the well-established methods to obtain consent do not identify the parent effectively. COPPA puts forth several

⁹³⁸ 3.2.5.3; 4.10.3; 5.5.10.

⁹³⁹ COPPA 16 C.F.R. § 312.5(c).

⁹⁴⁰ Kamala D. Harris, ‘Making Your Privacy Practices Public’ (California Department of Justice, May 2014) <https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf> accessed 30 March 2017.

⁹⁴¹ Title 6 Commerce and Trade Subtitle II Other Laws Relating to Commerce and Trade Chapter 12c. Online and Personal Privacy Protection.

⁹⁴² DOPPA § 1204C.

⁹⁴³ ‘Complying with COPPA: Frequently Asked Questions’ (Federal Trade Commission) <[https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Verifiable Parental](https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Verifiable%20Parental)> accessed 30 March 2017.

⁹⁴⁴ Children’s Online Privacy Protection Act 15 U.S. Code § 6501(9).

⁹⁴⁵ ‘Complying with COPPA: Frequently Asked Questions’ (Federal Trade Commission) <[https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Verifiable Parental](https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Verifiable%20Parental)> accessed 19 March 2017.

non-exhaustive options that can be applied by the website operator such as providing a consent form to be signed by the parent and returned via U.S. mail, fax, or electronic scan (also known as the 'print-and-send' method).⁹⁴⁶ None of these methods is reliable enough to prove the identity of the parent/legal guardian giving consent⁹⁴⁷ (see 1.2.4; 3.2.5.3, 3.2.5.7; see 4.3.3.2, 4.3.3.3 & 4.10.3; 5.5.10.2).

The law does not require operators to provide the parental consent method. Industry practice is also varied on requiring parental consent, making it difficult to know whether it is compulsory or not. When parents are asked to give consent by, suppose, an email, what is their understanding of this consent? Do they think that consent is being given to allow their child to play a game or is it to allow the videogame website to collect personal information from children? It is important that parents have knowledge of what they are consenting to because, otherwise, it will be a valid consent from the websites' point of view but a misinformed, involuntary piece of communication from the parents' side.

Websites were readily advising parents to educate children on digital privacy risks without realising that it is impossible for parents to constantly supervise their children. Website operators should rely on data protection principles of

⁹⁴⁶ Ibid.

⁹⁴⁷ 'FTC Grants Approval for New COPPA Verifiable Parental Consent Method' (Federal Trade Commission, 19 November 2015) <<https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>> accessed 19 March 2017. The FTC should invest in new forms of parental consent methods such as the 'face match to verified photo identification' (FMVPI); 'Children's Data Protection and Parental Consent' (Advertising Education Forum, October 2013) <<http://www.aeforum.org/gallery/5248813.pdf>> accessed 31 January 2017.

minimality,⁹⁴⁸ (see 3.2.3.3) transparency⁹⁴⁹ and purpose specification⁹⁵⁰ (see 3.2.3.2) to ensure safety for children's digital privacy⁹⁵¹ (1.2.4; 4.10.3; 5.5.10.2).

Legislative authorities should take note of the fact that a parental consent mechanism can be fraught with challenges just like any age verification and identity authentication technology.⁹⁵² It is very difficult to verify the identity of the person giving consent.⁹⁵³ According to COPPA, once parental consent is obtained, websites can collect information from children under 13 years of age.⁹⁵⁴ Parental consent should not be the sole mechanism whereby websites can blindly start collecting information from children. Instead, laws need to be implemented that will allow scrutiny of the purposes for collecting information from children.

⁹⁴⁸ Directive 95/46/EC Article 6(1)(c): The principle of minimality limits data collection to what is adequate, relevant and not excessive; Directive 95/46/EC Recital 28; EU GDPR 2018 Article 5(1)(c).

⁹⁴⁹ EU GDPR 2018 Recital 58 and Article 5(1)(a).

⁹⁵⁰ Directive 95/46/EC Article 6(1)(b): Under the principle of 'purpose specification', data should be gathered for a specified, legitimate and compatible purpose; EU GDPR 2018 Article 5(1)(b).

⁹⁵¹ 'ICO GDPR Guidance' (ICO 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017.

⁹⁵² Berin Szoka and Adam Thierer, 'COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech' (2009) 16(11) The Progress & Freedom Foundation.

⁹⁵³ Ibid.

⁹⁵⁴ Ibid.

Consent is a challenging concept and should not be relied on strictly to protect children’s digital privacy. It is argued that website operators should ensure that processing of children’s personal data is minimal⁹⁵⁵ (see 3.2.3.3) and for a specified purpose,⁹⁵⁶ (see 3.2.3.2) to ensure safety for children’s digital privacy⁹⁵⁷ (see 1.2.4; 4.10.3)

Table 26 considers the eleventh criterion, namely data subjects’ right to access their data.

6.2.10. Table 26 Criterion 11 – Players’ right to subject access requests

Criterion 11 – Players’ right to subject access requests
Washington State privacy laws – These do not provide rules on the rights of data subject access requests
COPPA – COPPA requires website operators to provide parents with a means to reviewing any personal information the collect online from a child ⁹⁵⁸
CalOPPA – If the operator has a process whereby users can review and request changes to their personal information that is collected through their website, they should provide a description of that process ⁹⁵⁹
DOPPA – If the operator maintains a process whereby users can review and request changes to their personal information collected by the website, then the operator should provide a description of that process ⁹⁶⁰

All websites entitled users to review their information (see 5.5.11.1). COPPA makes it compulsory for website operators to provide parents with the option to view and update their children’s data. CalOPPA and DOPPA both use the word ‘if’, which means

⁹⁵⁵ Directive 95/46/EC Article 6(1)(c): the principle of minimality limits data collection to achieve the purpose behind the collection.
⁹⁵⁶ Directive 95/46/EC Article 6(1)(b): Under the principle of ‘purpose specification’, data should be gathered for a specified, legitimate and compatible purpose.
⁹⁵⁷ ‘ICO GDPR Guidance’ (ICO, 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017. The Information Commissioner’s Office (ICO) published guidance on the requirements of consent under the EU GDPR 2018. It states that, if valid consent cannot be obtained, the principles of fair data processing should be relied upon as an alternative legal basis for processing.
⁹⁵⁸ COPPA § 312.6.
⁹⁵⁹ CalOPPA 22575 (b)(2).
⁹⁶⁰ DOPPA § 1205C (b)(2).

that the operator will have to describe the process of subjects reviewing their data 'if' there is such a process. The law should make it compulsory website operators to provide for subject access requests and facilitate parents with the right to review their children's data. Legislation should clearly define the instances where operators can refuse to comply with subject access requests. Words such as 'unreasonable' and 'disproportionate' should be avoided to allow room for more specific provisions.

6.3. Overview of findings of the study of privacy policies of online videogame websites governed by U.S. data privacy law

Some significant observations were made from the study of privacy policies of videogame websites governed by U.S. data privacy laws.⁹⁶¹ Even though data privacy laws provide for the presentation and prominence of privacy notices, these were not applied. The law must be streamlined on the exact features needed to distinguish the policy as well as the location of the notice, which should be at the top of the homepage. A Flesch reading score⁹⁶² of 100–90, or 'very easy to read', can be extended to videogame privacy policies which will be suitable for a grade 5 or 11-year-old child.

Without knowledge of the exact governing legislation, users are unaware of their rights and obligations. The specified legislation should provide a link to the main provisions in concise and easy terms so that users can furnish a more informed consent.

⁹⁶¹ Chapter 5 Table 5: *Dota 2, Clash of Clans, Minecraft, Pogo, Candy Crush Saga and Princess Isabella.*

⁹⁶² *Ibid.*

The websites collect extensive pieces of information from users, without clearly explaining the purpose for doing so. Methods to opt-out of data tracking should be simplified. There is no explanation for why users need to control their privacy settings.

It should be a legal requirement for websites to provide the exact method of obtaining parental consent and data subject access requests without employing vague reasons to defeat them.

Now that the criteria established in Chapter 5 Table 4 have been analysed against the data privacy rules of the U.S., in the following section the same criteria will now be evaluated against the data privacy rules in EU.

6.4. Videogame websites governed by European data privacy law

This section deals with the first and second criteria collectively because they are contained in the same provision in the European data privacy laws.

6.4.1. Table 27 Criterion 1 – Location of privacy policy – and Criterion 2 – Length and wording of privacy policy

Criteria 1 and 2 – Location of privacy policy and length and wording of privacy policy
Data Protection Directive 95/46/EC – Directive does not provide any rules on the location of privacy policy or wording/length of the policy.
e-Privacy Directive – User should be provided with ‘clear and comprehensive’ information in accordance with the Directive 95/46/EC about the purposes of processing. ⁹⁶³
EU GDPR 2018 – The regulation does not provide any rules on location or length of privacy policy. Information should be presented ‘in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.’ ⁹⁶⁴
Article 29 EU Data Protection Working Party – Privacy policy should be placed prominently, and information should be presented in a plain and simple manner that is easy to understand for children. ⁹⁶⁵

The privacy policies of nine videogame websites⁹⁶⁶ were located at the very bottom of the main webpage and lacked any distinguishing or prominent features.

The European data privacy laws focus on the conditions of processing data rather than the way the information is presented (see 3.2.3). The EU GDPR 2018 does not provide rules on the location of the privacy policy, a standard of readability or the appropriate length for the privacy policy. The e-Privacy Directive requires the

⁹⁶³ e-Privacy Directive Article 5(3).

⁹⁶⁴ EU GDPR 2018 Article 12.

⁹⁶⁵ Article 29 Data Protection Working Party, ‘Guidelines on transparency under Regulation 2016/679’ (Europa 11 April 2018) [file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018.

⁹⁶⁶ Chapter 5 Table 5: *Dota 2, Candy Crush Saga, Clash of Clans, Princess Isabella, Heroes of the Storm, Minecraft, Prince of Persia, Miniclip and League of Legends.*

operator to provide information in 'clear and comprehensive' terms without explaining the standard for clarity.

Art29 WP makes recommendations that privacy policies be placed prominently on the website using positioning and colour.⁹⁶⁷ It also provides guidance on the meaning of clear and concise, intelligible (*see 3.2.4.1*) and using plain language with respect to children (*see 3.2.4.2 & 3.2.4.3*). Although Art29 WP provides examples of good practice and to consider the UN Convention on the Rights of the Child in Child Friendly Language⁹⁶⁸ for child-centric language, but without a set standard of readability, website operators can devise their own interpretations of making the privacy policy child-friendly.

The same issue of prominence is observed in EU based videogame websites as the U.S. The U.S. data privacy law allows website operators a list of options to make the privacy policy prominent. But none of the privacy policies used these options (*see 6.2.1*). Art29 WP has advised website operators to employ positioning and colour to make the privacy policy prominent, but the privacy policies did not exhibit such features.

The EU GDPR 2018 requires information to be presented in clear and concise manner. There is limited guidance on how plain, clear or simple the information should be (*see 3.2.5.8*).

⁹⁶⁷ Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa 11 April 2018)
[file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Download/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Download/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018.

⁹⁶⁸ <https://www.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf> accessed 21 May 2018.

The Art29 WP⁹⁶⁹ and EU GDPR 2018 should provide a standard of readability such as the Flesch Reading score test for websites (*see 5.5.2.2 and 5.5.2.3; 6.2.2*). EU laws should further emulate the U.S. data privacy provisions on the presentation of privacy policies. At present, these are under the advisory jurisdiction of Art29 WP. Such recommendations should be made into laws.

Table 28 deals with the third criterion, governing legislation.

6.4.2. Table 28 Criterion 3 – Governing legislation

Criterion 3 – Governing legislation
Data Protection Directive 95/46/EC – The Directive regulates the processing of personal data within the European Union. Since it is a directive, it must be adopted by the European member states into their internal domestic law. ⁹⁷⁰ Therefore, even if the videogame website is governed by the laws of England and the Data Protection Act 1998 applied, it will contain the same principles as the Directive 95/46/EC transposed into the English legal system
e-Privacy Directive – The e-Privacy Directive is a continuation of Directive 95/46/EC and builds on consumers' digital rights by addressing new digital technologies ⁹⁷¹ such as cookies and third-party tracking technologies. This directive is transposed into the domestic legislation of member states and therefore will be applicable when considering the operation of cookies and tracking technologies
EU GDPR 2018 – The Regulation does not contain provisions on placing the governing law within the privacy policy.
Article 29 EU Data Protection Working Party – The Working Party does not provide any guidance on the laws governing privacy policies

Videogame privacy policies should specify the data privacy law and provide a link to a reputable source such as the Information Commissioner's Office (*see 5.4.1; 6.2.3.1*).

⁹⁶⁹ <<http://www.lawsociety.org.uk/news/stories/article-29-working-party-new-gdpr-guidance-notes/>> accessed 24 January 2018.

⁹⁷⁰ 'Complexity of EU Law in the Domestic Implementing Process' (Europa, 3 July 2014) <http://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf> accessed 31 March 2017.

⁹⁷¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

6.4.3. Criterion 4 – Privacy rules involving the Privacy Shield Framework to safeguard transfer of data between the EU and the U.S. – and Criterion 5 – TRUSTe privacy certification

The Privacy Shield Framework aims to safeguard transfer of data between the EU and the U.S. (see 5.5.4; 6.2.4). In the list of games governed by EU and U.S. law, only Pogo applies the framework. This could be because the framework may apply where data is transferred from EU to the U.S. Therefore, it will not be considered in this section.

Table 29 deals with the sixth criterion, namely collection of personal information.

6.4.4. Table 29 Criterion 6 – Collection of information from children

Criterion 6 – Collection of information from children
Data Protection Directive 95/46/EC – Personal data can be collected only for specified, explicit and legitimate purposes. ⁹⁷² The personal data must be adequate, relevant and not excessive with respect to the purposes for which the data is collected ⁹⁷³
e-Privacy Directive – It requires the website operators to follow the same data processing principles established in the Directive 95/46/EC ⁹⁷⁴
EU GDPR 2018 – The Regulation gives effect to the purpose limitation principle whereby personal data shall be collected for specified, explicit and legitimate purposes. ⁹⁷⁵ It also gives effect to the data minimisation principle whereby personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. ⁹⁷⁶
Article 29 EU Data Protection Working Party – It recognised the lack of legal certainty created by ‘legitimate interests’ (as a purpose of processing personal data), which can be susceptible to broad interpretations ⁹⁷⁷

The videogame websites create a distinction between what constitutes personal data and non-personal data. Directive 95/46/EC defined personal data as any information

⁹⁷² Directive 95/46/EC Article 6(1)(b); EU GDPR 2018 Article 5(1)(b).

⁹⁷³ Directive 95/46/EC Article 6(1)(c); Directive 95/46/EC Recital 28; EU GDPR 2018 Article 5(1)(c).

⁹⁷⁴ E-Privacy Directive Article 5(3).

⁹⁷⁵ EU GDPR 2018 Article 5(1)(b).

⁹⁷⁶ EU GDPR 2018 Article 5(1)(c).

⁹⁷⁷ ‘When Is Processing Personal Data in Your Legitimate Interests’ (Slaughter and May, 2014)

<<https://www.slaughterandmay.com/media/2162779/when-is-processing-personal-data-in-your-legitimate-interests.pdf>> accessed 15 March 2017.

related to an identified or an identifiable natural person (see 3.2.1; 5.5.6.1).⁹⁷⁸

Although there was no legal definition for what constituted non-personal data, when combined with another piece of information it can be used to identify, trace or locate a person⁹⁷⁹ by using device IDs,⁹⁸⁰ cookies⁹⁸¹ and IP addresses.⁹⁸²

Most devices use dynamic IP addresses⁹⁸³ and they change over time.⁹⁸⁴ In October 2016, the European Court of Justice ruled in *Patrick Breyer v Bundesrepublik Deutschland*⁹⁸⁵ that dynamic IP addresses will constitute personal data because they will comprise a ‘means likely reasonably to be used to identify’ the individual.⁹⁸⁶ Data privacy law should accept the possibility of non-personal data to become personal data and therefore extend its protection to the latter.

Directive 95/46/EC allowed data processing in certain circumstances such as for the performance of a contract.⁹⁸⁷ Data processing had to be for ‘specified, explicit and legitimate’ purposes⁹⁸⁸ and avoid vague reasons such as ‘improving user

⁹⁷⁸ Directive 95/46/EC Article 2(a); Michael Sweeney, ‘What Is PII, Non-PII, and Personal Data?’ (7Suite 7 September 2017) <<https://7suite.com/2016/09/what-is-pii-personal-data/>> accessed 1 April 2017.

⁹⁷⁹ EU GDPR 2018 Recitals 28 and 30.

⁹⁸⁰ ‘Device ID’ (Microsoft) <<https://docs.microsoft.com/en-us/windows-hardware/drivers/install/device-ids>> accessed 18 April 2018 A device ID is a string of numbers that identifies a smartphone or tablet anywhere in the world.

⁹⁸¹ Cookies are small text files that are downloaded onto a user’s computer or smartphone when they visit a website. It helps to remember users’ devices as well as store information about their preferences or past actions. ‘Cookies and Similar Technology’ (ICO) <<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>> accessed 18 March 2017.

⁹⁸² ‘Static v. Dynamic IP Address’ (Google fiber) <<https://support.google.com/fiber/answer/3547208?hl=en>> accessed 1 April 2017. An IP address is a unique number assigned to every device on a network; just as a street address determines the address the letter should be addressed to, the IP address identifies computers on the internet. Michael Sweeney, ‘What Is PII, Non-PII, and Personal Data?’ (7Suite 7 September 2017) <<https://7suite.com/2016/09/what-is-pii-personal-data/>> accessed 1 April 2017.

⁹⁸³ Dynamic internet protocol address (techopedia) <<https://www.techopedia.com/definition/28504/dynamic-internet-protocol-address-dynamic-ip-address>> accessed 18 April 2018. A dynamic IP address is a temporary IP address assigned to a computing device when it connects to the internet.

⁹⁸⁴ Ibid.

⁹⁸⁵ Judgment in Case C-582/14: *Patrick Breyer v Bundesrepublik Deutschland*.

⁹⁸⁶ Ibid.

⁹⁸⁷ Directive 95/46/EC Article 7.

⁹⁸⁸ Directive 95/46/EC Article 6(1)(b); EU GDPR 2018 Article 5(1)(b).

experience'⁹⁸⁹ (see 3.2.3.2). Eight videogame websites used terms such as 'improving the quality of our services', 'support advertising services' and 'deliver excellent experiences' as one of the purposes for collecting user data.⁹⁹⁰ This position has now changed, and some of the updated privacy policies avoid using such purposes to justify processing of data.

The EU GDPR 2018 has widened the definition of personal data because it includes 'online identifiers'⁹⁹¹ in the definition of personal data.⁹⁹² The EU GDPR 2018 has broadened principles of transparency,⁹⁹³ data minimisation⁹⁹⁴ (see 3.2.3.3), purpose specification⁹⁹⁵ (see 3.2.3.2 & 3.2.4), and strict consent requirements under the EU GDPR 2018 (see 3.2.5.5 & 3.2.5.6) that ensures children's personal data remains safe. These are helpful provisions because they treat children as a special class of data subjects. But the privacy policies are collecting extensive information from children in contravention of the data privacy laws.

⁹⁸⁹ Article 29 EU Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (Europa, 2 April 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 1 April 2017.

⁹⁹⁰ see 5.5.6; 6.2.6.

⁹⁹¹ Any identifier that you would use for the purpose of online communication. This would include a screen name if you posted in an online forum or a login you used for an application or website through which you communicate and can include email address, instant chat.<<https://floridaactioncommittee.org/question/internet-identifier-exactly-required-registered/>> accessed 10 December 2017.

⁹⁹² Frederik Zuiderveen Borgesius, 'Behavioral Targeting, a European Legal Perspective' (2013) 11(1) IEEE Security & Privacy 82, 82–85.

⁹⁹³ EU GDPR 2018 Recital 58 and Article 12 and 13. The Regulation requires controller to also furnish contact details of the data protection officer; the right to lodge a complaint with a supervisory authority; information about whether data is transferred to a third country; the legitimate interests pursued by the controller; and whether further processing will be required.

⁹⁹⁴ Directive 95/46/EC Article 6(1)(c): The principle of minimality limits data collection to achieve the purpose behind the collection.

⁹⁹⁵ Directive 95/46/EC Article 6(1)(b): Under the principle of 'purpose specification', data should be gathered for a specified, legitimate and compatible purpose.

Table 30 considers the seventh criterion, namely third parties collecting personal information.

6.4.5. Table 30 Criterion 7 – Third parties collecting personal information

Criterion 7 – Third parties collecting personal information
Data Protection Directive 95/46/EC – Third parties can process data when it is necessary for the purposes of pursuing their legitimate interests except where such interests are overridden by the interests of the data subject ⁹⁹⁶
e-Privacy Directive – It does not have any rules on third parties collecting personal information
EU GDPR 2018 – Processing is necessary for the purposes of the legitimate interests pursued by a third party, except where such interests are overridden by the interests of the data subject which require protection of personal data, in particular where the data subject is a child ⁹⁹⁷
Article 29 EU Data Protection Working Party – The Working Party does not provide guidance on third parties collecting personal information

The eight videogame websites allow third parties to collect personal information, but the privacy policy does not define the term ‘third party’. It has been defined legally in Directive 95/46/EC⁹⁹⁸ and the EU GDPR 2018⁹⁹⁹ as any person other than the data subject, controller and processor.

Third parties are allowed to process personal data to pursue their legitimate interests.¹⁰⁰⁰ The Art29 WP stated that third parties can have a legitimate interest in understanding their consumers’ preferences through forms of marketing as long as it is acceptable under the law.¹⁰⁰¹ The Art29 WP went on to state that this does not mean the operator will be allowed to collect extensive information from the user.

⁹⁹⁶ Directive 95/46/EC Article 7(f).

⁹⁹⁷ EU GDPR 2018 Article 6(f).

⁹⁹⁸ Directive 95/46 EC Article 2(f).

⁹⁹⁹ EU GDPR 2018 Article 6(f).

¹⁰⁰⁰ Article 29 EU Data Protection Working Party, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’ (Europa, 9 April 2014) http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm accessed 2 April 2017.

¹⁰⁰¹ Ibid.

Legitimate interests need to be clearly defined. Third parties should not have a legitimate interest in collecting personal information belonging to children. Terms such as ‘legitimate interests’ should be avoided as it can be interpreted broadly

Table 31 considers the eighth criterion, namely cookies and other tracking technologies.

6.4.6. Table 31 Criterion 8 – Cookies and other tracking technologies

Criterion 8 – Cookies and other tracking technologies
<p>Data Protection Directive 95/46/EC – According to the Art29 WP, since behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles, which, in most cases, will be deemed personal data, Directive 95/46/EC be applicable¹⁰⁰²</p> <p>e-Privacy Directive –According to the Working Party, advertising network providers are bound by Article 5(3) of the e-Privacy Directive, pursuant to which placing cookies or similar devices on users’ terminal equipment or obtaining information through such devices is only allowed with the informed consent of the users¹⁰⁰³</p> <p>EU GDPR 2018 – The Regulation extends the definition of personal data to include ‘online identifiers’ to identify an individual.¹⁰⁰⁴ Cookies are specifically included as personal data under the terms of the Regulations.¹⁰⁰⁵ Article 20 of the regulation will deal specifically with online profiling.</p> <p>Article 29 EU Data Protection Working Party – The Working Party does not question the economic benefits that behavioural advertising will bring for businesses, but it believes that the practices must not be carried out at the expense of individuals’ data protection and privacy rights¹⁰⁰⁶</p>

¹⁰⁰² Article 29 EU Data Protection Working Party, ‘Opinion 2/2010 on Online Behavioural Advertising’ (Europa, 22 June 2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf> accessed 18 April 2017.

¹⁰⁰³ Ibid.

¹⁰⁰⁴ EU GDPR 2018 Article 4(1).

¹⁰⁰⁵ EU GDPR 2018 Recital 26 & 30; Damian Clifford, ‘EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster – Tracking the Crumbs of Online User Behaviour’ (jipitec) <<https://www.jipitec.eu/issues/jipitec-5-3-2014/4095>> accessed 18 April 2017.

¹⁰⁰⁶ Article 29 EU Data Protection Working Party, ‘Opinion 2/2010 on Online Behavioural Advertising’ (Europa, 22 June 2010) <https://webcache.googleusercontent.com/search?q=cache:J1qvDBpz-SgJ:https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/junio/WP171en.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 18 April 2017.

Websites should limit the use of tracking technologies in videogame websites which can collect directly identifiable information belonging to the user.¹⁰⁰⁷

6.4.6.1. Article 5(3) e-Privacy Directive

Article 5(3) of the e-Privacy Directive¹⁰⁰⁸ refers to cookies and other technology that can store or gain access to information stored on the individual's terminal equipment.¹⁰⁰⁹ Behavioural advertising methods entail processing of personal data, engaging both the e-Privacy Directive and Directive 95/46/EC.¹⁰¹⁰

6.4.6.2. Prior consent under the e-Privacy Directive

There is a requirement of prior informed consent before cookies collect information from users,¹⁰¹¹ which should be valid, freely given, specific and an informed indication of the data subject's wishes.¹⁰¹² The privacy policies fail to meet this requirement because the simple act of entering the website is taken to amount to consent¹⁰¹³ (see 5.5.8). This e-Privacy Directive is to be replaced by the e-Privacy Regulation.¹⁰¹⁴ It will

¹⁰⁰⁷ Ibid. The Art29 WP on behavioural advertising states that the use of cookies will involve the processing of unique identifiers and the collection of IP addresses, which allows the tracking of particular machines (even where dynamic IP addresses are used). Secondly, information collected is related to users' characteristics and profiles can be linked with directly identifiable information given by the user.

¹⁰⁰⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

¹⁰⁰⁹ Article 29 EU Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (Europa, 22 June 2010) <https://webcache.googleusercontent.com/search?q=cache:J1qvDBpz-SgJ:https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/junio/WP171en.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 18 April 2017; e-Privacy Directive 95/46/EC Recital 24.

¹⁰¹⁰ Directive 95/46/EC Article 2.

¹⁰¹¹ e-Privacy Directive Article 2(f).

¹⁰¹² Directive 95/46/EC Article 4(11).

¹⁰¹³ Directive 95/46/EC Article 10.

¹⁰¹⁴ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

make giving cookie consent more user friendly as browser settings will become easier to accept or refuse cookie consent (*see 3.3*).

In the updated EU GDPR 2018 compliant privacy policies, the term ‘implied consent’ has been removed. In the EU GDPR 2018, consent must be in the context of a written declaration¹⁰¹⁵ (*see 3.2.5 and 3.2.5.5; 5.5.6.3*) Similarly, it should be easy to withdraw consent as it is to give consent.¹⁰¹⁶ This puts an obligation on website operators to define the different kinds of cookies used and the methods to disable them.

6.4.6.3. Users may not be able to alter their browser settings

Recital 66 of the amended e-Privacy Directive indicates that the user’s consent may be expressed by using appropriate settings for their browser. This shows that consent can be given in different ways. The Art29 WP cautions that, for valid consent to apply,¹⁰¹⁷ data subjects cannot be expected to have consented simply because they used a browser which by default enables the collection and processing of their information.¹⁰¹⁸ Data subjects are not always aware of how to alter their browser settings and disable cookies, even if this is included in privacy policies. It is wrong to expect that inaction by the data subject provides a clear and unambiguous indication of their wishes. The Art29 WP pointed out that the responsibility of using cookies cannot be limited to expecting the user for taking or not taking certain precautions in their browser settings.¹⁰¹⁹ Three out of four major browsers have a default setting to

¹⁰¹⁵ EU GDPR 2018 Articles 4(11) and 7(2).

¹⁰¹⁶ EU GDPR 2018 Article 7(3).

¹⁰¹⁷ Ibid.

¹⁰¹⁸ Article 29 EU Data Protection Working Party, ‘Opinion 2/2010 on Online Behavioural Advertising’ (Europa, 22 June 2010) <https://webcache.googleusercontent.com/search?q=cache:J1qvDBpz-SgJ:https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/junio/WP171en.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 18 April 2017.

¹⁰¹⁹ Paul Lambert, *A User’s Guide to Data Protection* (Bloomsbury Publishing Ltd 2016).

allow all cookies, which means that cookies are being sent and information is collected prior to obtaining consent, thus making the need for prior consent purposeless.¹⁰²⁰

Since cookies are personal data under the EU GDPR 2018¹⁰²¹, consent is required for cookies which is a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes.¹⁰²² For consent to be valid, information should be presented in a clear and intelligible manner (*see 3.2.5.8*).¹⁰²³

This has resulted in websites posting extensive information about the use and function of cookies in their privacy policy. An unintended consequence is the increased word length in privacy policies which is not child-friendly as children are expected to read lengthy documents.

Website privacy policies should limit the information contained in children's privacy policy. Information should be compatible with the reading abilities of children.

¹⁰²⁰ Ibid.

¹⁰²¹ EU GDPR 2018 Recital 30.

¹⁰²² EU GDPR 2018 Recital 32.

¹⁰²³ GDPR consent guidance (ICO) < <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/>> accessed 19 May 2018.

Table 32 deals with the ninth criterion, namely methods to disable cookies and other third-party tracking technologies.

6.4.7. Table 32 Criterion 9 – Methods to disable cookies and third-party tracking technologies

Criterion 9 – Methods to disable cookies and third-party tracking technologies
Directive 95/46/EC – There are no rules on methods to disable cookies and third-party tracking technologies
e-Privacy Directive – Recital 25 of the e-Privacy Directive provides that users should be given the opportunity to refuse to have a cookie or similar device stored on their terminal equipment
EU GDPR 2018 – Recital 66 of the amended e-Privacy Directive indicates that the user’s consent may be expressed by using the appropriate settings of a browser or other application, ‘where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC’
Article 29 EU Data Protection Working Party – The Article 29 Working Party is of the view that prior opt-in mechanisms, which require an affirmative data subject’s action to indicate consent before the cookie is sent to the data subject, are more in line with Article 5(3) ¹⁰²⁴

6.4.7.1. Opting out of tracking is not an easy process

Legal guidance falls short of the method whereby users can refuse to have cookies installed on their terminal equipment.¹⁰²⁵ The page for opting out of cookies was framed in technical language. When users fail to opt out, they have impliedly made an informed decision to allow tracking of their data. Since consent is assumed rather than specific, it does not meet the requirements of consent under the now repealed Directive 95/46/EC. The Art29 WP does not consider the opt-out mechanism to provide average users with effective means of consent to being profiled.¹⁰²⁶

¹⁰²⁴ Article 29 EU Data Protection Working Party, ‘Opinion 2/2010 on Online Behavioural Advertising’ (Europa, 22 June 2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf> accessed 20 April 2017.

¹⁰²⁵ Ibid.

¹⁰²⁶ Ibid.

The updated privacy policies provide methods to opt-out of cookies. These are not simple to follow because they expect users to consult their browser documentation; read privacy policies of third parties and the methods to disable cookies; and unsubscribe links in email correspondence (see 5.5.9.1).

Websites should obtain valid consent from users and give clear instructions on how to alter their browser settings rather than simply ask them to consult their browser documentation.

Table 33 deals with the next criterion, namely the parental consent mechanism.

6.4.8. Table 33 Criterion 10 – Parental consent mechanism

Criterion 10 – Parental consent mechanism
Data Protection Directive 95/46/EC – The Directive does not provide any specific rules on processing children’s personal data, and rules on children’s ability to consent to such processing. The Directive does not make a distinction between data subjects of varying ages
e-Privacy Directive – The Directive does not provide any rules on processing children’s personal data
EU GDPR 2018 – Article 8 of the regulations limit children’s ability to consent to data processing without parental authorisation. Previously, the rule set the age of consent at 13 years but, after the last round of trilogue negotiations, ¹⁰²⁷ the final draft decided for the age of consent to be 16 years, though it also allows member states to set a lower age not below 13 years of age. ¹⁰²⁸
Article 29 EU Data Protection Working Party – The Working Party advises data controllers and processors that they should provide children’s data a high level of protection. ¹⁰²⁹ The Working Party provides general information on regarding the best interests of a child but does not specify any particular binding rules.

At present, the European directives do not provide any specific set of rules that regulate the processing of children’s personal data. The EU GDPR 2018 achieves a

¹⁰²⁷ ‘EU Data Protection Reform: Where Are We – and What Can You Do to Prepare?’ (Olswang) <http://www.olswang.com/media/48316310/olswang_s_top_12_eu_data_protection_reform.pdf> accessed 22 April 2017.

¹⁰²⁸ EU GDPR 2018 Article 8(1).

¹⁰²⁹ Article 29 EU Data Protection Working Party, ‘Working Document 1/2008 on the Protection of Children’s Personal Data (General Guidelines and the Special Case of Schools)’ (Europa, 18 February 2008) <<http://www.dataprotection.ro/servlet/ViewDocument?id=358>> accessed 22 April 2017.

milestone by introducing new rules for children as data subjects.¹⁰³⁰ But there are outstanding questions such as when parental consent should be sought. How can operators prove the identity of the parent/guardian? Yet, there have not been any submissions on the possible methods to obtain parental consent. It is recommended that alternative forms of data processing should be used that rely on principles of minimality,¹⁰³¹ (see 3.2.3.3) transparency and purpose specification¹⁰³² (see 3.2.3.2) to ensure safety for children's digital privacy¹⁰³³ (see 1.2.4; 4.10.3; 5.5.10.2; 6.2.9).

The EU GDPR 2018 should aim to achieve harmony by fixing the age of consent at 18 years. The Art29 WP should provide guidance on the best forms of the parental consent mechanism which will allow businesses to adopt standards already set and give parents the clarity in knowing how they will consent.

¹⁰³⁰ EU GDPR 2018 Article 8(2). The data controller is required to make 'reasonable efforts' to verify that consent has been obtained from the holder of parental authority taking into consideration available technology; 'Children's Data Protection and Parental Consent' (Advertising Education Forum, October 2013) <<http://www.aeforum.org/gallery/5248813.pdf>> accessed 22 April 2017. The law does not specify how parental consent will be implemented and delegates to the European Commission, which will invite member states to put forth their contributions on a valid parental consent mechanism.

¹⁰³¹ Directive 95/46/EC Article 6(1)(c): the principle of minimality limits data collection to achieve the purpose behind the collection.

¹⁰³² Directive 95/46/EC Article 6(1)(b): Under the principle of 'purpose specification', data should be gathered for a specified, legitimate and compatible purpose.

¹⁰³³ 'ICO GDPR Guidance' (ICO, 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017.

Table 34 considers the eleventh criterion, namely players' right to subject access requests.

6.4.9. Table 34 Criterion 11 – Players' right to subject access requests

Criterion 11 – Players' right to subject access requests
Data Protection Directive 95/46/EC – Article 12 of the Directive provides that data subjects will be allowed to obtain from the data controller access to their data
e-Privacy Directive – It does not provide any rules on subject access requests
EU GDPR 2018 – The EU GDPR 2018 deals with data subjects' right of access under Article 15

Vague reasons can be used to deny subject access requests, if they are unreasonably repetitive or require disproportionate effort (*see 5.5.11.1*).¹⁰³⁴ The Court of Appeal stated in *Dawson-Damer v Taylor Wessing LLP (2017)*¹⁰³⁵ that 'disproportionate effort' must involve more than an assertion that it is too difficult to search through voluminous papers.

The law does not explain the mechanism whereby data subjects can request to obtain personal data. The law should provide guidance on how this right can facilitate children and their parents to access their data or request to have it changed.

Having analysed both the U.S. and EU data privacy laws in respect of the 11 criteria to evaluate privacy policies of the 10 videogame websites, the following section will provide an overview of the preliminary findings.

¹⁰³⁵ [2017] EWCA Civ 74.

6.5. Legal analysis of the study of privacy policies of the videogame websites governed by EU data privacy laws

Law should provide for privacy policies to be prominently placed, preferably on top of the webpage, exhibiting distinguishing features, and governing law should indicate the specific choice of law for purposes of clarity and transparency.

The EU GDPR 2018 admits that online identifiers (IP Address, E-mail address etc) can be combined with other information to identify natural persons¹⁰³⁶ (see 5.5.6.1). Therefore, website privacy policies should acknowledge that if personal and non-personal data are used together, it can be used to identify an individual. Similarly, laws should define a 'third party', require that their purposes for data collection be clearly explained and place limits on the information they can collect from users.

Individuals have to give prior informed consent to the use of tracking technologies.¹⁰³⁷ Under the EU GDPR 2018, consent has to be a clear, informed choice in a written context.¹⁰³⁸ Data subjects should be able to withdraw their consent at any time.¹⁰³⁹ Since an affirmative action will be sought for each aspect of data collection, it is unclear how these onerous measures will apply to children and their parents. Methods to disable cookies should arguably be a single click. Clash of Clans presented the simplest method to opt-out via a single click. However, in the updated privacy policy, clicking the opt-out button on the Clash of Clans website takes the user

¹⁰³⁶ EU GDPR 2018 Recitals 28 and 30.

¹⁰³⁷ e-Privacy Directive Article 5(3).

¹⁰³⁸ EU GDPR 2018 Articles 4(11) and 7.

¹⁰³⁹ EU GDPR 2018 Article 7(3); EU GDPR 2018 Article 4 and Recital 32.

to the third-party privacy policy. The user is then expected to follow the method posted by the third party to disable tracking (*see 5.5.9.1*).

Laws should be altered to require websites to specify the method of parental consent mechanism and additional guidance is needed on the use of data subject access requests.

Strengthening EU institutions that regulate data privacy

In the EU, the European Data Protection Supervisor (EDPS),¹⁰⁴⁰ data protection authorities¹⁰⁴¹ and the Art29 WP should have the authority to enforce EU GDPR 2018 (*see 4.7 and 4.10.4*), just like the FTC can enforce COPPA (*see 4.3.3.5*) and U.S. state attorneys (*see 4.4.2*).

The study has considered the data protection and privacy legislation that regulates the videogame website's privacy policies in each of the chosen legislatures. This was followed by a detailed evaluation to discuss the compatibility of the practice of privacy policies with existing law and the expectation for children to read, understand and give their consent.

6.6. Conclusions and recommendations

Privacy policies give key details on the relationship between the website operator and user by describing the data handling practices of the website. A problem can occur if a videogame website attracts users of all ages, including a large younger

¹⁰⁴⁰ European Data Protection Supervisor' (Europa) <https://edps.europa.eu/about-edps_en> accessed 19 August 2017.

¹⁰⁴¹ Directive 95/46/EC Article 28. The European data protection supervisory authority will be established for each member state and assist in complying with the provisions of the Directive by providing guidance to the government and initiate legal proceedings if there is a violation of the principles of Directive 95/46/EC.

audience, and the privacy policy is structured for an adult user. Children might not read the privacy policy if they are inclined to play the game. Children should be facilitated to read, understand and consent to the terms of the privacy policy.

6.6.1. Privacy policies are lengthy and dense legal documents

The privacy policies of 10 videogame websites were lengthy documents, using complicated terms and requiring users to read the policies of third-party links they click on, which effectively adds to the word length. Data privacy law fails to provide a standard of prominence, location, readability and length of the privacy policy.

The legal guidance provided by Art29 WP¹⁰⁴² sets out broad principles for data protection law. For example, data controllers can have different legitimate interests in the processing of personal data. The Art29 WP further broadens the concept by stating the notion of legitimate interests can comprise a multitude of interests such as freedom of expression or information, direct or other forms of marketing, advertisement etc.¹⁰⁴³ It would be helpful to provide additional guidance on specific data privacy issues such as the prominence and exact location of the privacy policy or the standard of readability, which will make it easier for children and their parents to read and understand its terms. The Art29 WP recognises that children need special protection and that principles on data quality should be adapted to suit their interests.¹⁰⁴⁴ Website operators should act with the utmost good faith when

¹⁰⁴² <<http://www.lawsociety.org.uk/news/stories/article-29-working-party-new-gdpr-guidance-notes/>> accessed 24 January 2018.

¹⁰⁴³ Ibid.

¹⁰⁴⁴ Article 29 EU Data Protection Working Party, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (Europa 11 February 2009) <http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=2&hl=en&ct=clnk&gl=uk> accessed 14 April 2018.

processing their personal data.¹⁰⁴⁵ The Art29 WP fails to explain the meaning of ‘good faith’ or the circumstances that will amount to ‘good faith’.

CalOPPA requires the privacy notice to be posted on the homepage,¹⁰⁴⁶ without specifying which part of the page. As a result, the privacy policy was posted at the bottom of the page, which was difficult to locate. Similarly, the law provided a choice in the list of distinguishing features¹⁰⁴⁷ to highlight the privacy notice. The policies did not employ any of these features. It is stated that laws should make it incumbent upon websites to employ at least one of these distinguishing features.

The privacy policies that have not been updated continue to imply consent when the user enters the website or uses its services. Under the EU GDPR 2018, consent is a positive and affirmative action.¹⁰⁴⁸ It is unclear how children and their parents will provide affirmative consent upon every aspect of data collection. Consent should be a positive and well-informed action, undertaken by the user after having read and understood information that is presented to them in easy-to-understand language, which coincides with their reading and understanding abilities.

If a solution is found for the above issues, difficulties can still be encountered: if the privacy policy is not prominently displayed and hence hard to locate on the main webpage; if the document is too long, uses complicated language, uses privacy frameworks, collects extensive information from the user without clearly explaining the purpose for doing so; or if consent is implied and it fails to indicate a specific piece

¹⁰⁴⁵ Ibid.

¹⁰⁴⁶ CalOPPA 22577(b)(1).

¹⁰⁴⁷ CalOPPA 22577(b)(2).

¹⁰⁴⁸ EU GDPR 2018 Article 4 and 7.

of law/legislation that users can refer to if they are wronged. In Chapter 5, it was found that these issues still exist and must be resolved for children to use the videogame websites by exercising informed choices.

6.6.2. Governing legislation

The research found that the governing law is contained in the terms and conditions of the website under the heading 'Governing legislation'. None of the terms of service mentioned the specific legislation that was applicable. There was a general reference to the applicable laws as the 'laws of Washington State' or 'laws of England' (contained in the terms and conditions) but not an exact indication of the specific data protection and privacy laws that will apply. It is customary practice to refer broadly to the contractual law in the terms of service (5.4.1). This thesis recommends that privacy policies should contain the governing privacy law to inform users of the website's data handling practices as well as the law that will apply if a dispute arises between the parties. Instead of users carrying independent research to retrieve the governing law, the privacy policy should provide a link to a reputable source such as the Information Commissioner's Office (ICO) in England that contains the governing data privacy law. Otherwise, only individuals with a legal background will be able to find the law that will apply to the privacy policy (*see 5.4.1 & 6.2.3.1*).

The website needs to specify the choice of law because different countries apply different laws and therefore varying levels of digital privacy. In disputes involving websites, various state parties can be involved. Owing to the varying degrees of online protection in different countries, it is imperative that the governing law is clearly set out from the beginning. In the case of Washington State, U.S.A, a myriad

of statutes deals with an individual's right to privacy. As a result, the research could not pinpoint any law that governed the terms of the privacy policy. Lack of knowledge of the law meant that readers are not aware of the rights and obligations they are legally entitled to. Therefore, it is recommended that the specific law should be mentioned, and this information should be contained in the privacy policy as well.

6.6.3. Privacy frameworks such as TRUSTe privacy certification and the Privacy Shield Framework

Regulatory bodies need to rethink the inclusion of privacy frameworks such as TRUSTe privacy certification and the Privacy Shield Framework, which are criticised for their lack of effectiveness in protecting individuals online as they do not have clear eligibility criteria, have voluntary status, have an unclear purpose and expect users to go to the homepage and explore the rules for themselves. It is insisted that the privacy policy should only contain information that will help the user make informed decisions rather than burden them with additional reading material.

6.6.4. Collection of personal information, third parties collecting information and opt-out mechanisms

All the websites collect extensive information from users. At present, laws in the U.S., the EU and Canada do not specify the level of information that should be collected from children. Data privacy laws should be amended to provide strict guidelines on the information that can be collected and compatible with the age of the user. Websites should be required to give exact and specified reasons for collecting data. Law needs to put in place a universal opt-out mechanism which is simple and easy to follow. Simply being asked to consult one's browser settings does not facilitate users

when they are a child. This displays a lack of responsibility for the user's privacy on the part of the website.

6.6.5. Parental consent mechanism

Apart from *Prince of Persia*, none of the websites provided for a method of parental consent. There was no indication of the responsibilities expected from parents when their children interact with the online community. Laws should require websites to clearly describe the method of parental consent for the benefit of parents/guardians. Legal authorities should also understand that parental consent mechanism, like any identity authentication technology, can pose challenges. Therefore, a parental consent mechanism on its own should not allow website operators to collect data from children. Other mechanisms such as explicit and specified purposes for collection should also be relied on.

6.6.6. Data subject's right to access their information

All the websites allowed the user the right to access, correct and/or delete their information. It is not clear whether this right would be of use to children, who may not find it important to correct their information. Websites need to explain the right of data subject access requests (SARs) in simple terms. It should explain why it is important for users to amend their data if needed and what can happen if they don't amend it. Websites should not use wide-ranging terms as reasons for rejecting requests such as if they are 'unreasonably repetitive', 'required disproportionate technical effort', 'jeopardize the privacy of others' or 'are extremely impractical'. How many repeat requests would amount to 'unreasonably repetitive'? Wouldn't repeat

requests signify urgency on the part of the user to alter their personal information held by the website? The website should avoid such wide-ranging terms or explain what they mean.

This chapter discussed the data protection and privacy laws that are operable in the EU, the U.S. and Canada. It involved a two-part comparative multiple case study analysis that considered the adequacy and effectiveness of data privacy laws that regulate each criterion (*Chapter 5 Table 4*). The findings from the study were also considered with respect to the ability of children to read, understand and give consent to the privacy policies. During the outcome of the analysis, recommendations were made on how the law can be altered to provide greater protection to children's digital privacy rights. The two-part multiple case study carried out in Chapters 5 and 6 was essential in delivering an understanding on the current industrial practice of the use of privacy policies in videogame websites. It was beneficial in detailing whether the practice is commensurate with the reading and understanding abilities of children under 18 years. The legal study provided an evaluation of whether data privacy laws sufficiently regulate privacy policies and whether they can enforce the law upon deviating organisations. It also assessed whether the law considers the best interests of children and whether it adequately protects their digital privacy rights.

The two-part multiple case study has revealed worrisome findings, which will be addressed in the next chapter. Chapter 7 will address and identify gaps through an original child-friendly model privacy policy that also incorporates the findings of Chapters 5 and 6. Chapter 7 will carry out a brief case study of three interactive

children's gaming websites¹⁰⁴⁹ as benchmark to inform the child-friendly model privacy policy.

¹⁰⁴⁹ Disney, Harry Potter and BBC CBeebies.

CHAPTER SEVEN

ORIGINAL CHILD-FRIENDLY MODEL PRIVACY POLICY

7.1. Introduction

Chapters 1 to 6 evaluated the adequacy of data protection and privacy laws in protecting children's digital privacy rights. A comparative legislative analysis and a two-part multiple case study of the privacy policies of 10 popular videogames was undertaken. The study examined two main questions. Firstly, does the privacy policy comply with governing law? Secondly, do the practice of privacy policies and the governing data privacy law remain commensurate with the expectation that children should read, understand and consent to them?

This chapter is the main contribution to this thesis. The detailed study carried out in the previous chapters has uncovered worrying findings with regards to protecting children's digital privacy. In addition to reading lengthy complicated documents, some privacy policies imply consent, so children will be assumed to have consented upon entering the website. They are expected to find out for themselves how the method to disable cookies. The study uncovers important limitations between children's interaction with websites and the practice of privacy policies and governing data privacy laws that should protect children's data and keep them safe.

This chapter will carry out a mini case study of the privacy policies of three children's online interactive gaming websites. Disney.com, Harry Potter (www.warnerbros.co.uk), and cbeebies.co.uk as benchmarks to inform the child-

friendly model privacy policy. Some examples of best practices treat children as a special class of data subjects such as a separate children's privacy policy; specifying the governing data privacy law at the start of the privacy policy; and a privacy policy that is easy to read and understand.

The original child-friendly model privacy policy will address the gaps identified in the study. It will facilitate children and their parents with informative guidance in brief and easy-to-understand language. It will use a Flesch reading score of 100–90, which means that it can easily be read by an 11-year-old child or a grade 5 student. The policy will avoid using privacy frameworks, which only tend to confuse readers; methods to disable cookies will be a simple click that will be indicative of the user's wishes. The policy will refrain from using links that can be clicked to open complicated documents with unclear instructions on how to opt out of cookies. The method for obtaining parental consent will be provided for parents' convenience. The privacy policies in the study did not mention the governing law. The child-friendly model privacy policy will provide the specifically applicable governing law. In addition, it will provide a short and easy-to-understand version of the main principles of the governing law so that children and their parents can understand the rights and obligations they are entitled to.

Chapter 7 Section 7.2 draws on developments in online privacy policies used by interactive entertainment organisations: the Disney Corporation, BBC CBeebies and Harry Potter (collectively referred to as 'DBH privacy policies') at the forefront of child-friendly privacy policy information to inform the recommendations for the videogame industry. The study of the DBH privacy policies will act as a benchmark

and inform both recommendations and best practices to draft a child-friendly model privacy policy in Section 7.7. Each website privacy policy will be analysed based on the 11 criteria established in Table 4.

7.2. Study of privacy policies as benchmarks to guide the original child-friendly model privacy policy

Three privacy policies of child-oriented online websites were selected: Disney.com¹⁰⁵⁰, CBeebies¹⁰⁵¹ and Harry Potter¹⁰⁵², for their popular association with children's games. The privacy policies were studied to determine whether they address the shortcomings observed in the multiple case study carried out in Chapters 5 and 6. The findings of this comparative analysis can establish guidelines that will help draft the child-friendly model privacy policy.

Disney.com was selected for the mini case study because it is popular amongst children worldwide. Since it primarily caters to children, it is expected to keep abreast of latest technological and legal developments to protect children's digital interests when they use Disney.com. The study of Disney.com can provide useful information regarding the data gathering practices of popular children's gaming websites and possibly make significant contributions to the child-friendly model privacy policy.

¹⁰⁵⁰ <www.disney.com/> accessed 27 October 2017. After the EU GDPR 2018 came into effect on 25th May 2018, clicking on www.disney.com would take the user to a regional Disney website namely www.disney.co.uk.

¹⁰⁵¹ <https://www.bbc.co.uk/cbeebies> accessed 27 October 2017.

¹⁰⁵² Harry Potter <<https://www.warnerbros.co.uk/games/harry-potter-spells>> accessed 31 May 2017.

7.3. Overview of Disney.com privacy policy

Disney.com is the official website for Disney, which includes theme parks, movies, TV programmes, games, shopping etc.¹⁰⁵³ Disney Games is a free-to-play videogame website with a wide variety of games based on Disney characters and movies.¹⁰⁵⁴ The following paragraphs discuss the privacy policies of Disney Games, examining each of the 11 criteria (*Chapter 5 Table 4*).

The privacy policy was updated when studied on a second occasion after 25th May 2018 when the EU GDPR 2018 came into effect. The following criteria will discuss any changes observed.

7.3.1.1. Use of language

Disney Games has furnished two privacy policies: a ‘Primary Policy’ that informs the general audience about its data handling practices and a separate ‘Children’s Privacy Policy’ that deals specifically with the collection, use and sharing of children’s data. Both policies are worded in easy-to-understand English with definitions provided for difficult terms. Information about cookies and third-party tracking was formulated in technical terms. It is not clear if Disney is implementing a standard for readability of the policy such as the Flesch reading test (*see 5.5.2.3; 6.2.2, 6.4.1*).

7.3.1.2. Children’s Privacy Policy

Creating a separate privacy policy that deals with the data privacy of children is a welcome addition. The policy only applied to children under 13 years of age, which

¹⁰⁵³ <www.disney.com/> accessed 27 October 2017.

¹⁰⁵⁴ <<http://games.disney.co.uk/>> accessed 27 October 2017.

coincides with the protections offered by COPPA. Both law and privacy policy ignored children between the ages of 13–17 years. COPPA should incorporate similar provisions as the DOPPA¹⁰⁵⁵ and extend protection for children up to 18 years.

The Children’s Privacy Policy was tediously long, with a word count of 2,489 words, which was additional to the 2,917 words contained in the Primary Policy. Information about cookies and tracking technologies was contained in other documents that added extensively to the existing word limit. The Children’s Privacy Policy was not an independent document and had to be read in conjunction with the Primary Policy, which meant that users had to read much more than was contained in the privacy policy document.

7.3.1.3. Governing legislation

On Disney.com, the Children’s Privacy Policy stated at the very outset that it complies with COPPA. The policy also provided a link to the text of COPPA for the user’s reference. This information is helpful for children and their parents because they can find out the rights and obligations they are entitled to under the privacy policy. It would be helpful if the Children’s Privacy Policy could provide a short and simple read of the main provisions of COPPA for children and their parents’ reference.

7.3.1.4. Privacy frameworks

An irregularity in the use of privacy frameworks – the Privacy Shield Framework and the TRUSTe certification seal – was also observed in the Disney website. The

¹⁰⁵⁵ Title 6 Commerce and Trade Subtitle II Other Laws Relating to Commerce and Trade Chapter 12c. Online and Personal Privacy Protection.

Children's Privacy Policy utilised the TRUSTe logo, which could be clicked to access the TRUSTe homepage, which had additional documents. Such frameworks will have little value for parents and their children and should be avoided in the children's privacy policy.

7.3.1.5. Collection of information from the user

Disney Games provided an exhaustive list of information collected from users. The website used the umbrella term 'information' to refer to personal and non-personal data. This shows that Disney Games appreciates the possibility of non-personal data being used alongside personal data to identify the individual. The list was concise and explained in easy terms.

Consent was required as an affirmative and positive action upon each and every instance, when personal data was collected.

7.3.1.6. Cookie and other tracking technologies

The outlay of the cookie policy was very different from the rest of the website. The cookie policy did not follow the same simple pattern as the rest of the privacy policy. The Disney website explained cookies and other tracking technologies in detail. There are links which can be clicked for additional information. The method to opt out from cookies was confusing, littered with technical language and difficult to follow. Rather than facilitating the user, it made the process to disable cookies complicated, which in turn would discourage users from doing anything about their privacy settings. To disable cookies, one single click should be sufficient (*see 5.5.9.1*).

The updated privacy policy had a separate cookie policy placed on the front page of the website. It explained the various kinds of cookies used by the website including flash cookies. The document was lengthy and explained cookies in simpler terms. Methods to opt-out involved clicking on links and following complicated instructions which is not child-friendly.

7.3.1.7. Parental consent method

It was proposed that videogame website privacy policies should provide a valid parental consent mechanism (*see 5.5.10.2*). The Children's Privacy Policy provided the different methods of parental consent. This is useful information because parents would now be able to know what form of consent will need to be given and whether they prefer this method. If they have any queries, they are given contact details which they can deliver their questions to.

Best practices observed in the Disney.com privacy policy was a separate children's privacy policy that cater's to the informative needs of children and their parents. It also presents the governing data privacy law and provides a link for users to click on and read. The methods to opt-out of cookies are complicated even though the cookie policy was introduced after the EU GDPR 2018 came into effect, but the cookie policy does not cater to the new law.

The next section will carry out a mini case study of CBeebies privacy policy. This is a regional UK based popular children's gaming website. EU is a frontrunner in data privacy law and the study of popular UK based children's gaming website will highlight the compatibility of commercial data gathering practices with the law.

7.4. Overview of the [bbc.co.uk/cbeebies](https://www.bbc.co.uk/cbeebies) privacy policy

CBeebies is a free online website that provides games and activities for children.¹⁰⁵⁶

Below is a study of the privacy policy of CBeebies games, examining each of the 11 criteria for evaluating privacy policies (*Chapter 5 Table 4*).

The privacy policy was presented in a child-friendly manner. This is because the privacy policy used easy-to-understand language. The policy was divided into questions such as 'What's in this policy?' which is answered in bullet points rather than paragraphs. The privacy policy does not specify a standard of readability, but it does employ simple language. But the document was very lengthy containing 3161 words. It is recommended that privacy policies should not only be easy to read, they should also be short and brief.

The privacy policy provides vague reasons for collecting data such as 'plan and improve our services.' Purpose for collecting data should be specific and compatible with digital privacy interests of children. The privacy policy does not specify parental consent or the age at which it is required. Additional guidance is provided in the document titled 'how can I keep my children safe online?' but it is difficult to flesh out the method for parental consent. This should be provided in the main privacy policy.

Cookies were dealt with in the same privacy policy. The use and function of cookies was presented in easy to understand and brief words. Disabling cookies was simplest by swiping a button.

¹⁰⁵⁶ CBeebies <<https://www.bbc.co.uk/cbeebies>> accessed 30 May 2017.

The best practice of the CBeebies privacy policy was presentation of information in bullet points which was brief and easy to understand. The method to opt-out of cookies was very child-friendly with a simple swipe of the button. Providing guidance to parents with regards to protecting their children's data is informative and should be encouraged in children's videogame websites.

The next section will conduct a mini case study of the Harry Potter website privacy policy. The reason behind choosing Harry Potter is that it is a popular worldwide children's website that is owned by the U.S. and popular amongst users including the EU. This study can provide useful information in demonstrating whether children's gaming websites connected to multiple regions can protect children's digital privacy in accordance with the laws of the land.

7.5. Overview of the Harry Potter website (www.warnerbros.co.uk) privacy policy

Harry Potter is an online website owned by Warner Brothers.¹⁰⁵⁷ The website provides information about movies distributed by Warner Brothers as well as online videogames inspired by the Harry Potter film series. Below is a study of the Harry Potter website privacy policy, while examining the 11 criteria for evaluating privacy policies. The privacy policy was updated on 10 May 2018 which will also be included the study below.

The Harry Potter website presented the reader with a short privacy policy comprising 489 words. This policy had to be read in conjunction with the other general policy,

¹⁰⁵⁷ Harry Potter <<https://www.warnerbros.co.uk/games/harry-potter-spells>> accessed 31 May 2017. The privacy policy was updated on 10 May 2018.

comprising 3,701 words. It was a useful practice to present the main points briefly and allow users the choice to read additional information in the general policy, located below in the same document.

The updated privacy policy had an increased word length of 4765 words which is lengthy and extensive for children to read.

The governing legislation was contained in the terms of use and vaguely referred to local laws rather than the laws of a particular jurisdiction. Amongst the study of videogame website privacy policies, the governing legislation of Harry Potter website was most uncertain. What is meant by 'local laws'? Users are expected to retrieve the location of the registered office and then assume the laws pertaining to that area.

Third parties play an active role on the Harry Potter website and collect extensive information from children. It is difficult to reconcile with the digital privacy interests of children.

Method to disable cookies was very simple. Cookie policy was contained on the front page and the user could disable cookies with a swipe of the button. This was both child-friendly and easy to use.

7.6. Best practices obtained from the study of the DBH privacy policies

The study of the DBH privacy policies carried out in Sections 7.2–7.4 found material differences with the findings of the study of privacy policies in Chapters 5 and 6.

Wording and presentation of privacy policies

Firstly, the latter used easy-to-understand terms and difficult words were explained in simple words and on the same page for easy access. The original child-friendly model privacy policy will use similar language. Difficult terms, if any, are explained on the same page to prevent users from having to click on links to read additional documents. The child-friendly model privacy policy will substitute difficult words with easier terms to avoid adding definitions, which would make the document long and tedious to read.

The website privacy policy should add from the outset that if users have any questions about the privacy policy they should contact the website operator. The website should use an automated message box rather than provide a postal address or email, which is more difficult to operate.

The policy will be an independent document that can easily be read by children. It will follow the Flesch reading test with a score of 90–100 so that it can easily be read by children aged 11 years or grade 5. The privacy policy will ideally have a word count of 400–800 words. The privacy policy is aimed at children between the ages of 16 – 18 years but it is written for children aged 11 years. The reason is to maximise chances of understanding. Parents/legal guardians of all abilities will be able to discuss the implications of the privacy policy with their children while fully understanding the terms. For example, comic books have different age-rating but they all correspond to

a Flesch Reading score of 90 to 100 (easy to read for a child in 5th grade)¹⁰⁵⁸ to enhance comprehension.

Separate child-friendly model privacy policy

Disney.com presented the user with a separate privacy policy that specifically dealt with the website's data handling practices of children. It is proposed that a website should have a separate child-friendly privacy policy. The children's privacy policy in Disney.com was not an independent document and had to be read alongside the general privacy policy. Additionally, the policy detailed the data handling practices for children under 13 years of age only. Children under 18 years were still treated as adults and had to read the general policy to understand and consent to Disney.com's data handling practices. The child-friendly model privacy policy will adopt the practice of a separate privacy policy for children, as in Disney.com.

Choice of applicable law

Disney.com mentioned the specific choice of law that will apply to the terms of the privacy policy.¹⁰⁵⁹ This is useful information as it informs the website users about the data privacy rights they are entitled to under the legislation. It can be appreciated that children may not have the legal background to understand the terms of the law used and the protection it offers.

The privacy policy should facilitate parents and children to understand the rights and obligations by providing a link to a reputable source that contains the governing data

¹⁰⁵⁸ Stewart, J., 'Recalibrating the Flesch Readability Index for the Twenty-first Century' <http://www.academia.edu/30700337/Recalibrating_the_Flesch_Readability_Index_for_the_Twenty-first_Century> accessed 16 November 2018.

¹⁰⁵⁹ see 5.4.1 and 5.5.3; 6.2.3, 6.4.2 and 6.6.2.

privacy law. The child-friendly model privacy policy will provide the specific choice of law as the governing legislation at the outset. There will be a link that opens a short document, which is brief and is easy to read and simple and explains the main provisions of the legislation applicable to the privacy policy.

TRUSTE privacy certification

It was observed that, apart from Disney.com (Children’s Privacy Policy), there is no mention of the Privacy Shield Framework or TRUSTe privacy certification. It is maintained that their presence complicates the document and will be avoided.

Collection of information from children

The DBH privacy policies listed six to seven broad categories of information they collect. Examples are provided for the information that falls under each category. This is good practice as it explains to the user what information is collected from them. To aim for a simple child-friendly model privacy policy, the information should be presented in succinctly brief and plain terms. Examples will be provided regarding collection of information and respective uses without using technical terms. Third parties will be introduced, explaining the information they collect and the purpose of their collection in brief and easy-to-understand terms. Users will not be expected to read the privacy policies of third parties. It is asserted that the host website bears the responsibility to ensure that it monitors and regulates the privacy practices of third parties operating on its website. The host website should protect the data privacy interests of its users and make sure that third-party privacy practices remain compatible with those of the host website.

Methods to disable cookies

Harry Potter and Cbeebies presented the simplest method to disable cookies. A single swipe could disable cookies instead of opting out hundreds of third parties operating on the website or consult one's browser documentation. Previously Clash of Clans presented the most preferable method to disable cookies,¹⁰⁶⁰ where three clicks allowed the user to opt out.

It is also believed that website privacy policies should do more to inform users about the importance of altering their privacy settings. At present, the choice to disable cookies is presented in neutral terms. The child-friendly model privacy policy will inform users that, if they are worried about their privacy owing to the online tracking methods, they can disable cookies.

The child-friendly model privacy policy will explain cookies in simple terms and avoid detailed explanations of the other tracking methods used by the website. The child-friendly model privacy policy will avoid using too many links, which is a clever way to hide the actual word length of the policy.

The concept of consent is not applied stringently in all the privacy policies studied for this thesis. Consent should be an informed choice on the part of the user and website operators should not imply it. Under the EU GDPR 2018, it is an affirmative, clear and unambiguous action by the user.¹⁰⁶¹ It is for these reasons that the research proposes

¹⁰⁶⁰ Before Clash of Clans privacy policy was subjected to an update which will become effective on 25 May 2018.

¹⁰⁶¹ EU GDPR 2018 Articles 4 and 7.

asking the user at the end of the policy that, if they have read, understood and agreed to the terms of the privacy policy, they should click on 'I agree'.

This study has presented the findings of the multiple case study of 10 privacy policies and considered the data protection and privacy laws in the U.S., the EU and Canada that regulate them. Proposals have been made for best practices for future videogame website privacy policies and recommendations for legal amendments to current and prospective data privacy laws. The DBH privacy policies were considered in making further recommendations and obtaining best practices to inform the child-friendly model privacy policy.

Below is the original child-friendly model privacy policy which is the main contribution to this thesis. It should be noted that the model privacy policy has not been drafted in consultation with children. It is intended that the child-friendly model privacy policy will be read, understood and legitimately consented to by users including children of videogame websites. It will be assumed that the child-friendly model privacy policy belongs to *Dota 2*.

7.7. Original child-friendly model privacy policy

ORIGINAL CHILD-FRIENDLY MODEL PRIVACY POLICY

This Privacy Policy will tell you what information Dota 2 collects about you; how it collects the information and the companies it shares the information with. If you have any questions about this privacy policy, click on this [link](#) to message your query.

It is important that you read, understand and consent/agree to this Privacy Policy before you begin to play Dota 2.

Dota 2 applies the Flesch Reading Score of 100.0–90.0. It means that this privacy policy is easy to read for an 11-year-old child. It is governed by the [U.S. Children's Online Privacy Protection Act \('COPPA'\)](#). Click on the link to find out about your rights and obligations under this Act.

Collection of Information

The information Dota 2 collects includes your name, email address, the country where you live, the credit/debit card number used for purchasing products/services on this website, your likes and dislikes and how often you use this website.

You should be very careful when sharing your information online. We stress that you do not share your information publicly in places like the multiplayer chat or multiplayer game play where strangers can easily look at your information.

Use of Information

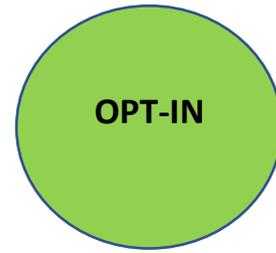
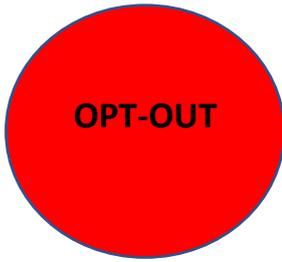
Dota 2 will use the information to recognise you; to continue to deliver games that you enjoy playing; and to send you information about events and contests if you have subscribed to them. We will share your information with companies connected to Dota 2. These companies are also called 'third parties'. If you visit the 'third-party' website by clicking on links contained on Dota 2, these companies will use your information to recognise you and advertise games that they find will be of interest to you. Dota 2 will also reveal your information for legal reasons such as court orders.

Children under the Age of 16

If you are under 16, you will be asked to provide your parent or guardian's email address. They will be contacted to obtain their consent and validate your use of Dota 2. If we do not receive a verifiable parental consent within 72 hours, we will require a signed consent form by mail, email or fax or require your parent/guardian to speak to a trained customer service representative by telephone or video chat.

Cookies and Other Technologies to Collect User Information

Cookies are small 'text files' that are downloaded onto your device. Its purpose is to remember information about you. For example, it will remember you when you visit Dota 2. Both Dota 2 and its third parties will use cookies to collect information about you. If you are concerned about your privacy and you are not happy for us to collect information about you, you can disable cookies by clicking on the opt-out button. If you decide to change your preference, you can click on the opt-in button.



Access, Correcting, Deleting Your Information

We would advise you to contact us if you want to access, correct and/or delete your information. We will inform you if it is not possible to comply with the request such as if processing your request would disclose information about another Dota 2 game player. You will have the right to appeal our decision. You can contact us by clicking [here](#).

If you have read and understood the terms of this Privacy Policy, click on the Agree Button to express your consent/agreement.



THE END

Word count – 562

7.8. Changes proposed in the child-friendly model privacy policy

In the child-friendly model privacy policy ('MPP'), this study has proposed significant changes to address the shortcomings that were observed in the multiple case study carried out in Chapters 5 and 6. The privacy policies were using moderately complicated terms including technical and legal jargon. It was found that lengthy documents and difficult terminology were used when the policy dealt with privacy frameworks (TRUSTe privacy certification and the Privacy Shield Framework), third-party tracking technologies and methods to disable them. The MPP avoids the use of difficult legal and technical terms, which is believed to have little use for the user and makes the document unnecessarily long and complicated. While it encompasses all the components of a traditional privacy policy, it aims to explain all these components in very easy-to-understand English for the benefit of users.

The MPP has incorporated the Flesch reading test as a standard to measure the readability of the policy. The MPP addresses the user as 'you' rather than 'user' as a form of direct reference.

Another observation in the multiple case study was an average word length of up to 4,000 words. It is an unrealistic expectation by website operators that users, especially children, will both read and understand them. The MPP substantially reduces the word length to 562 words and expects that the drastically shorter version will encourage users to read and easily understand the privacy policy.

The uncertain terms of the governing legislation were another observation that added to the vagueness of the privacy policies studied in Chapters 5 and 6. The

Children’s Privacy Policy on Disney.com states at the very outset that the policy will be governed by COPPA and adds a link that users can refer to, for their understanding of the law. The MPP has also included the governing legislation (COPPA) in the beginning of the privacy policy, which is attached as Annex 1 at the end of Chapter 8. The law has been hyperlinked, which can be clicked on to access the provisions of COPPA. Unlike on Disney.com, where the link opens on to a document that contains the entire COPPA, the link in the MPP facilitates a brief version of the law (255 words), which provides the main provisions of COPPA in easier terms.

The study in the earlier chapters revealed the extensive information collected from users. *Minecraft* was collecting a remarkable 36 pieces of information. Vague reasons were given as purposes for collecting the information, such as ‘to improve user experience’. The MPP dismisses the use of such vague terms. It has not included the complete list of information to be collected from users. Instead, it has mentioned the most recognisable pieces to the user without creating a distinction between personal and non-personal data. The MPP recognises that non-personal data can become personal data if coupled together. This is in accordance with the requirements of the EU GDPR 2018, which has for the first time recognised that online identifiers can be used to identify individuals.¹⁰⁶²

Unlike the privacy policies observed in the multiple case study, which rarely mentioned the parental consent mechanism, the MPP duly includes a verifiable

¹⁰⁶² EU GDPR 2018 Recitals 26 and 30.

parental consent method in a separate paragraph. This will benefit both children and parents in knowing the form of consent method used from the outset.

In the multiple case study, third-party tracking technologies and methods to disable cookies were framed in difficult terms and contained links to third party privacy policies or one had to opt-out of several data tracking mechanisms. Little understanding exists for users to go through this complicated process and disable cookies. The terms of the MPP inform users of the possibility of a privacy invasion by stating 'If you are concerned about your privacy...'. Similarly, the process of disabling cookies is a simple click on the same page rather than visiting another document and opting out of several third-party websites. It is believed that such practices would make the entire process of tracking and disabling technologies simpler and easier to apply.

This is also in line with the requirements of the EU GDPR 2018. Processing of data is based on consent in the context of written declaration. The request for consent should be provided in clearly distinguishable, intelligible and easily accessible form.¹⁰⁶³ It must also be easy to withdraw consent as it is to give it.¹⁰⁶⁴ This means that even if an individual has opted out of tracking, it should still be possible for them to change their preference and opt-in. For these reasons, the MPP explains the function of cookies in clearly legible terms. The data subject is provided with the option to opt-out as well as opt-in to cookies.

¹⁰⁶³ EU GDPR 2018 Articles 4 and 7 and Recital 42.

¹⁰⁶⁴ EU GDPR 2018 Article 7(3).

The MPP informs the user that they have a right to access, correct and/or delete information. In the multiple case study, access requests could be declined if they are ‘unreasonably repetitive’, ‘required disproportionate technical effort’, ‘jeopardize the privacy of others’, or ‘are extremely impractical’. These are very vague reasons for declining requests. For instance, how many repeat requests would amount to ‘unreasonably repetitive’? The MPP removes reasoning that can give the website operator a plethora of ways to decline requests. The only reasonable way in which requests can be declined is if revealing of the information would disclose data relating to other users. Rather than asking users to email or call the website operator for the information request, the MPP uses an automatic message box.

Most importantly, consent in the MPP is based on a positive and informed action by the user. The user is required to click on the ‘Accept’ button after having read the privacy policy. This is in accordance with the requirement of EU GDPR 2018, that consent should be given ‘in the context of a written declaration’¹⁰⁶⁵ (see 3.2.5.5). The MPP does not presuppose or infer consent by a simple act of the user entering the website or using its services.

Privacy policies list the website’s data handling practices. When users consent to the terms of the privacy policies, their data will be collected, processed and shared with third parties in accordance with the terms of the privacy policy. This process should be explained to users in easy-to-understand language. Only then could users provide informed consent that signifies their clearly considered choices. Videogame websites

¹⁰⁶⁵ EU GDPR 2018 Articles 7(2).

should be aware of the large volume of young users. It should provide a privacy policy that coincides with the reading and understanding abilities of children.

The MPP is beneficial on several grounds as discussed above and could be adopted by videogame websites as a guide for drafting children's privacy policy. The MPP addresses several key findings in both the multiple and mini case study conducted in Chapters 5, 6 and 7. The MPP is exclusively designed for children and treats them as a special class of data subjects.

7.9. Recommendations and conclusions

It was found that websites typically presume users to have a pre-existing understanding of legal terms, that they can consult their browser documentation and alter the privacy settings. This thesis drafts an original child-friendly model privacy policy that provide children and their parents with a brief narrative of the terms and conditions of privacy policies. The aim is that it will be a first step in the direction towards facilitating children and their parents in understanding data handling practices of websites.

Videogames do not normally facilitate users with a separate child-friendly privacy policy. Some videogames updated their privacy policies in compliance with the EU GDPR 2018 and introduced a separate children's privacy policy. But this is lengthy and should be read in conjunction with the main policy. The child-friendly model privacy policy will serve as excellent and essential guidance for videogame developers and website operators to introduce privacy policies exclusively for children and their parents.

The research carried out in this thesis will be significant to developments aimed at safeguarding children from digital advertising and profiling. The study will facilitate legislators, game developers and those working with privacy policies to understand how data protection laws regulate data gathering practices within the EU, the U.S., and Canada. Most importantly, it provides how children can be treated as a special class of data subjects.

The child-friendly model privacy policy will facilitate legislators in formulating rules that are compatible with data handling practices directed towards children. For instance, the child-friendly model privacy policy applies a Flesch Reading Score of 100.0–90.0 which means that it can be read by an 11-year old child and comprises of 562 words. In view of this, legislators should draft laws requiring privacy policies directed towards children to be brief and employ a set reading standard. The child-friendly model privacy policy will also assist the courts (particularly in the EU) and website operators in determining whether data gathering practices comply with data privacy laws.

Digital literacy curriculum

Since children are expected to read, understand and consent to privacy policies, it is vital that they are introduced to digital literacy early on. A House of Lords Committee drafted a report stating that digital literacy should be introduced as a core subject alongside English and maths in the school curriculum in primary and secondary schools.¹⁰⁶⁶ It will furnish children with the requisite skills, knowledge and

¹⁰⁶⁶ 'Lords Say Digital Skills Will Make or Break the UK' (www.parliament.uk 17 February 2015) <<https://www.parliament.uk/business/committees/committees-a-z/lords-select/digital-skills-committee/news/report-published/>> accessed 9 March 2018;

understanding from an early stage, so that they can take an active role in intellectual life while protecting themselves online from private and commercial interests. Based on such notions, the child-friendly model privacy policy will be ideal in stimulating children to read documents framed in easy to understand language.

Article 12 of the United Nations Convention on the Rights of the Child makes it incumbent on policymakers that children's opinions be heard in matters that are important to them. If children are digitally literate, they can contribute towards decisions that affect their rights and interests. The child-friendly model privacy policy will help children in understanding websites' data handling practices. These children can actively participate and make well-informed contributions towards the drafting of privacy policies, videogame website's data gathering practices and the development of data protection and privacy laws that will treat children as a special class of data subjects.

The next chapter is the final chapter of this thesis. It will present the main key findings of this study as well as the recommendations made with respect to protecting children's digital privacy rights.

Cassie Hague and Sarah Payton, 'Digital Literacy across the Curriculum' (Futurelab, 2010) <<https://www.nfer.ac.uk/publications/FUTL06/FUTL06.pdf>> accessed 2 February 2018. According to Europe's Digital Agenda, 'digital literacy' or 'e-skills' are crucial to children's use of the internet. Sonia Livingstone and others, 'Digital Literacy and Safety Skills' (EU Kids Online) [http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20\(2009-11\)/EUKidsOnlineIIRReports/DigitalSkillsShortReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2009-11)/EUKidsOnlineIIRReports/DigitalSkillsShortReport.pdf) accessed 2 February 2018.

CHAPTER EIGHT

CONCLUSION

8.1. Introduction

*'The principle of best interest requires a proper appreciation of the position of the child. This involves recognising two things. First, a child's immaturity makes them vulnerable, and this must be compensated by adequate protection and care. Second, the child's right to development can only be properly enjoyed with the assistance or protection of other entities and/or people.'*¹⁰⁶⁷

Data protection law applies to children and adults alike. Children should be able to understand the law that applies to them and the consequences of providing consent to privacy policies (see 5.5.2.4). Data protection authorities should have stronger enforcement powers, with websites held accountable for non-compliance (see 4.10.4).

The Art29 WP recognised the need to provide children with adequate protection and care.¹⁰⁶⁸ Whereas data protection and privacy laws have typically been designed for adults, allowing children to be treated as adult data subjects.¹⁰⁶⁹ The problem is that children as a group are often neglected in legal research.¹⁰⁷⁰ Research into legal

¹⁰⁶⁷ EU GDPR 2018 Recitals 38 and 75; Article 29 EU Article Data Protection Working Party, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (Europa, 11 February 2009)

http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=2&hl=en&ct=clnk&gl=uk accessed 14 April 2018.

¹⁰⁶⁸ Ibid.

¹⁰⁶⁹ The Data Protection Directive 95/46/EC does not contain any provisions on treating children as a special class of data subjects. Data Protection Directive 95/46/EC.

¹⁰⁷⁰ Many medicines routinely used in children have not been formally evaluated by the system because the pharmaceutical industry is reluctant to study medicines in children. Sharon Conroy and others, Drug Trials in Children: Problems and the Way Forward (2000) 49(2) BJCP 93.

capability,¹⁰⁷¹ which is referred to as a persons' understanding of law-related issues and the ability to deal effectively with them, has focused primarily on adults and not children.¹⁰⁷² Children's digital privacy is a substantial concern for everyone, but policymakers have yet to include children's say in this regard (*see 5.5.2.4*). The uncertainty in interpreting consent and the inconsistent application of age for consent has caused further difficulties. For instance, in Germany the data controller will have to judge effective consent by looking at the degree of maturity exhibited¹⁰⁷³ by the child¹⁰⁷⁴ (*see 3.1.2*). What are the criteria for maturity and how is it defined by law? Children may be susceptible to digital privacy risks and should be treated as a special class of data subjects that require a high level of digital protection (*see 1.1*).

The final chapter of this thesis has four goals:

1. It will reflect on the findings of the comparative legislative analysis of the data privacy legislation in the EU, the U.S. and Canada (*Chapters 2–4*).
2. It lists the key observations made in the multiple case study of the privacy policies of 10 videogames (*Chapters 5 and 6*).
3. It determines if privacy policies adhere to the data protection and privacy laws that regulate their data handling practices. If the practices of privacy policies and governing laws are reasonable in expecting children to access, read, understand and consent to them. This analysis was carried out in Chapters 2–7. It explored children's experience generally across the use of videogames.

¹⁰⁷¹ 'Legal capability' is a term used by Dr Dawn Watkins in the article Dawn Watkins and others, Exploring Children's Understanding of Law in Their Everyday Lives (2018) 38(1) Legal Studies.

¹⁰⁷² Dawn Watkins and others, Exploring Children's Understanding of Law in Their Everyday Lives (2018) 38(1) Legal Studies.

¹⁰⁷³ Norbert Nolte and Christoph Werkmeister, 'Data Protection in Germany: An Overview' (Practical Law) <<http://uk.practicallaw.com/3-502-4080>> accessed 15 May 2016.

¹⁰⁷⁴ *Germany, Case No. 11 LC 114/13*.

4. It provides an original child-friendly model privacy policy based on the legislative analysis and multiple case study carried out in previous chapters (*Chapter 7*). The aim is that privacy policies should be brief and easy to read and understand for children and parents.

Finally, this chapter discusses the limitations of the study and reflects on recommendations for future topics to study. In summary, key problems uncovered are that privacy policies are lengthy, dense and complicated legal documents, difficult to locate on the website's homepage; there is no universal governing legislation that regulates the data handling practices of the website. The consent to policies permit the collection of extensive information from users without clearly defining the purpose for doing so; methods to disable cookies are difficult to implement; and the methods to provide verifiable parental consent are unreliable. This is exacerbated when dealing with children.

8.2. Key issues of the research

Chapters 3 and 4 carried out a legislative analysis of the data protection and privacy regimes of the EU, the U.S. and Canada to regulate data handling practices. The comparative legislative analysis of the data privacy laws of the EU, the U.S. and Canada made several findings. There is inconsistent application of children's age for consent in different jurisdictions; conditions to validate children's consent are unclear; there is uncertainty and lack of accountability in data privacy law; and there should be stronger enforcement powers for EU data protection authorities.

8.2.1. Varying ages for consent in different jurisdictions

Online consent is a rough-edged concept, partly because of the unclear conditions that need to be met to validate it. The first purported difficulty that the doctrinal legal research found was the varying ages for consent in different jurisdictions (*see 1.2.3; 3.1.2; 4.10.1*). This is a worrisome issue for children's digital privacy rights because data protection laws extend beyond borders. A videogame may be registered in one country, with a subsidiary organisation located in a different country and a child user accessing it from yet another country (*see 3.1.2*). A 16-year-old videogame player will be treated as a child in the UK¹⁰⁷⁵ but an adult in Germany, where the age of consent is 14 years.¹⁰⁷⁶

The earlier Directive 95/46/EC did not distinguish between children and adult data subjects (*see 3.2.5.2*). The lack of a uniform age at which children could provide consent resulted in EU member states adopting their own subjective interpretations for the age of consent (*see 1.2.3.; 3.1.2*). The EU GDPR 2018 came into force on 25th May 2018 in European member states,¹⁰⁷⁷ aiming to ensure harmonised application of EU laws, give greater protection and rights to individuals, and make the law compatible with new technology.

¹⁰⁷⁵ Ibid.

¹⁰⁷⁶ Carlo Piltz, 'The European Data Protection Law and Minors – No Legal Certainty' (German IT Law, 2014) <<http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty/>> accessed 12 January 2017.

¹⁰⁷⁷ 'Reform of EU Data Protection Rules' (Europa) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 16 May 2017.

The EU GDPR 2018 has for the first time treated children as a special class of data subjects.¹⁰⁷⁸ It has identified that children may be less aware of the online privacy risks.¹⁰⁷⁹ Information relating to data processing should be presented in a clear and plain language which should resonate with children and they recognise the message that is directed to them (*see 3.2.4*).¹⁰⁸⁰

The EU GDPR 2018 has classed children under 16 years but EU member states have the discretion to lower the age limit to 13 years,¹⁰⁸¹ which can defeat the purpose of achieving uniformity and certainty (*see 1.1 & 1.2.3; 3.1.2*). The U.S. also presents an inconsistent application of the ages at which children can provide legal consent, (*see 4.10.1; 1.2.3*) whereas Canadian data privacy law has not specified any provisions on children furnishing online consent.

It is recommended that a universal approach is adopted where all jurisdictions agree that anyone under the age of 18 years is defined a child (*see 1.2.3; 4.10.1*). However, it is unreasonable to subject 18-year-olds to parental consent methods. For this purpose, verifiable parental consent should be applicable to children under 16 years of age (*see 1.2.3; 3.1.2; 4.10.1*).

It seems that Brexit will have limited impact for the EU GDPR 2018 (*see 1.1.2*). The EU GDPR 2018 applies extraterritorially and will extend to non-EU member states as well.

¹⁰⁷⁸ EU GDPR 2018 Recital 58 and Article 12 and 13. The Regulation requires controller to also furnish contact details of the data protection officer; the right to lodge a complaint with a supervisory authority; information about whether data is transferred to a third country; the legitimate interests pursued by the controller; and whether further processing will be required.

¹⁰⁷⁹ EU GDPR 2018 Recital 38.

¹⁰⁸⁰ EU GDPR 2018 Recital 58; Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa 11 April 2018)

[file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018.

¹⁰⁸¹ EU GDPR 2018 Article 8.

Since the EU GDPR 2018 has allowed member states the discretion to lower the age of consent from 16 to 13 years,¹⁰⁸² the UK Data Protection Act 2018 has agreed for the age of consent at 13 years.¹⁰⁸³ Different member states may opt different ages for consent creating uncertainty in the law. It is hoped that in the future, the EU GDPR 2018 will agree on a universal age for consent. Similarly, the EU GDPR 2018 should also provide rules that regulate drafting and prominence of privacy policies, presentation of governing law and readability standard for privacy policies directed towards children. In other words, it should aim to treat children as a special class of data subjects.

8.2.2. Conditions to validate children's consent are unclear

The second issue uncovered by the legislative analysis was the difficulty in obtaining free and informed consent from children (*see 3.2.5; 4.10.1 and 4.10.3*). Consent is a core principle of data protection law (*see 3.2.5*). It is one of the several legal grounds that justifies the processing of personal data.¹⁰⁸⁴ Obtaining consent to process personal data may be a convenient legal basis for processing. But consent is not a straightforward concept, especially since the conditions for effective consent were unclearly defined by the now repealed EU Directive 95/46/EC (*see 3.2.5.2*). The EU GDPR 2018 requires consent in the context of a written declaration.¹⁰⁸⁵ It should be easy to withdraw consent as it is to give.¹⁰⁸⁶ This means that websites cannot imply

¹⁰⁸² EU GDPR 2018 Article 8.

¹⁰⁸³ Data Protection Act 2018 Section 9(a).

¹⁰⁸⁴ Directive 95/46/EC Article 7.

¹⁰⁸⁵ EU GDPR 2018 Articles 4(11) and 7(2).

¹⁰⁸⁶ EU GDPR 2018 Article 7(3).

consent anymore. And consent will have to be obtained upon every aspect of data collection (*see 1.2.3; 3.2.5.5, 5.5.6.2 and 5.5.6.3*).

The current identified consent methods offer limited protection to children (*see 3.2.5.2; 4.10.1 & 4.10.3; 5.5.6.2*). In view of the difficulties of getting children to have an appropriate level of understanding of what they are consenting to, parents are authorised to provide consent and validate their children's participation in the gaming website.¹⁰⁸⁷

The EU GDPR 2018 and U.S COPPA require website operators to obtain 'verifiable parental consent' from parents and legal guardians to allow the processing of children's personal data (*see 4.3.3.2 and 4.3.3.3; see 3.2.5.3 and 3.2.5.7*). The Federal Trade Commission has provided a non-exhaustive list of parental consent mechanisms that can be employed to obtain consent¹⁰⁸⁸ (*see 4.3.3.2*). The difficulty with these methods is that it is never certain if the person attempting to verify their identity is the parent/legal guardian (*see 4.10.3*). Children can provide a false age or create a fictitious email to do away with such formalities.¹⁰⁸⁹

Children and their parents should understand and appreciate the implications of giving legal consent. An unambiguous consent can be provided for a single processing activity such as subscribing for a newsletter, but it will be harder to demonstrate if the user consents to a privacy policy that will validate processing of data for multiple purposes (*see 1.2.4*). The EU GDPR 2018 adopts strict rules for consent¹⁰⁹⁰ (*see*

¹⁰⁸⁷ See 1.2.4; 3.2.5.3 and 3.2.5.7; 4.10.3; 5.5.10.2; 6.2.9, 6.4.8 and 6.6.5.

¹⁰⁸⁸ Federal Trade Commission, 'Protecting Kid's Privacy Online Reviewing the COPPA' (Federal Trade Commission, 2 June 2010) <<https://www.ftc.gov/news-events/events-calendar/2010/06/protecting-kids-privacy-online-reviewing-coppa-rule>> accessed 12 May 2017.

¹⁰⁸⁹ see 3.2.5.3; 4.3.3.3; 5.5.10.2.

¹⁰⁹⁰ EU GDPR 2018 Article 4(8).

3.2.5.5–3.2.5.8). This means that the processing of data can occur when the data subject has given consent in the ‘context of a written declaration’.¹⁰⁹¹ This will translate into constant pop up messages that can lead to consent fatigue¹⁰⁹² (*see 1.2.4; 3.2.5.5*).

It is recommended that there should be a uniform age for consent (18 years) and 16 years for obtaining verifiable parental consent (*see 1.2.3; 4.10.1*). Industrial practice needs to make sure that users understand the consequences of giving consent (*see 5.5.2.4*). This includes a separate child-friendly privacy policy that is prominently displayed and easy to understand. The privacy notice should clearly state the data collected from users, specify the purpose behind collection, and specify if the website is disclosing data to third parties (*see 5.5.2–5.5.7*).

Regarding the identification issues in verifiable parental consent methods, the Federal Trade Commission and the European Data Protection Supervisor should invest in innovative forms of consent mechanisms that ensure it is the parent/guardian giving consent.¹⁰⁹³ Alternatively, website operators should rely on the data privacy principles of minimality (*see 3.2.3.3*) and purpose specification (*see 3.2.3.2*) to ensure safety for children’s digital privacy (*see 4.10.3; 6.2.9*).

8.2.3. Certainty and accountability of the law

The doctrinal legal analysis (*see 1.6.2*) of the data protection and privacy laws of the EU (*Chapter 3*), the U.S. and Canada (*Chapter 4*) revealed a third issue: the uncertainty

¹⁰⁹¹ EU GDPR 2018 Articles 4(11) and 7(2). 6 out of 10 privacy policies were updated in late 2017 and 2018. The rest are still applying earlier rules on consent

¹⁰⁹² Christine Jolls and Cass R. Sunstein, ‘Debiasing through Law’ (2006) 35(1) *The Journal for Legal Studies* 199, 212.

¹⁰⁹³ Chapter 4 Section 4.3.3.5; Chapter 5 Section 5.5.10.2; Chapter 6 Section 6.2.9.

and lack of accountability of data privacy law (*see 4.10.2*). As technical possibilities for automated processing of data from multiple sources continue to grow, data protection law has become the crucial point of legal discussion.¹⁰⁹⁴

The trouble with data privacy law is the legal and practical uncertainty and accountability for economic operators and private users of online websites (*see 4.10.2*). For instance, U.S. COPPA fails to define ‘websites directed towards children’, and website operators and app developers will find it difficult to know if COPPA will apply to them (*see 4.3.3.1*). Similarly, some U.S. states such as Washington do not have a specific data privacy law (*see 4.6*). This is worrisome because children will be unaware of the law that governs the terms of the privacy policy.

Furthermore, principles for transferring data from the EU to the U.S. are unclear and lack accountability.¹⁰⁹⁵ After the annulment of the Safe Harbour Framework,¹⁰⁹⁶ (*see 3.2.6; 5.5.3*) the current Privacy Shield Framework has been criticised for not being robust enough¹⁰⁹⁷ (*see 5.5.4*). It is difficult to hold the website accountable for transferring personal data if the privacy framework principles and the eligibility criteria are unclear (*see 5.5.3 & 5.5.4; 6.2.4, 6.4.3 & 6.6.3*).

¹⁰⁹⁴ Bert Jaap-Koops, ‘The Trouble with European Data Protection Law’ (2014) 4(4) *International Data Privacy Law*.

¹⁰⁹⁵ Chapter 3 Section 3.2.6; European Data Protection Supervisor ‘Privacy Shield: More Robust and Sustainable Solution Needed’ (Europa, 30 May 2016)

<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 14 March 2017.

¹⁰⁹⁶ *Judgment in Case C-362/14 Maximilian Schrems v Data Protection Commissioner*.

¹⁰⁹⁷ European Data Protection Supervisor ‘Privacy Shield: More Robust and Sustainable Solution Needed’ (Europa, 30 May 2016)

<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 14 March 2017.

8.3. Comparative findings between legislation in the EU, the U.S. and Canada

The findings of the multiple case study revealed that videogame privacy policies are not designed for children. They are lengthy documents that lack the method for parental consent, collect extensive information. The child-friendly model privacy policy addresses these findings by being brief, easy to understand, presents the applicable law, method to disable cookies is a single click and consent is an affirmative act. The comparative legislative analysis has revealed important findings that the U.S. leads on provisions to protect children's digital privacy and rules on the practice of privacy policies, and regulatory bodies such as the Federal Trade Commission and California Attorney General playing an active role in shaping data privacy law (*see 4.4.2, 4.7, 4.10.4 and 4.11*). But, in terms of actual safeguards, EU appears to have stronger legal provisions (*see 4.7*).

It was found that U.S. data privacy laws treat children as a special class of data subjects to some extent. This is because there are laws specifically designed to protect the digital privacy rights of children (*see 4.3.3 and 4.5*). COPPA has fixed the age of consent at 13 years, whereas DOPPA defines anyone as a 'child' under 18 years.¹⁰⁹⁸ The U.S leads interms of legal requirements that regulate the prominence and content of privacy policies. Such rules were not observed in the earlier Directive 95/46/EC. The EU GDPR 2018 has made considerable progress by classifying children as under 16-year olds (*see 1.2.3; 3.1*) that require special protection (*see 3.2.4*). But the presentation, prominence and readability of privacy policies is in the form of guidance provided by Art29 WP (*see 3.2.4.1, 3.2.4.2 & 3.2.4.3*) which has advisory

¹⁰⁹⁸ Ibid.

status only. It is recommended that principles regarding the above should be introduced in the EU GDPR 2018 (*see 4.10*). There should be a universal standard of readability for privacy notices (*see 5.5.2.2 & 5.5.2.3; 6.2.2*). This would bring the legal requirements in line with treating children as a special class of data subjects. It will begin to form the basis of universal legal norms of data and privacy laws relative to children.

While, the comparative analysis suggests that the U.S. leads in children's data privacy law, in fact it is the EU GDPR 2018 that provides detailed definitions on all aspects of data privacy law (*see 3.2.1; 4.11*). The EU has stronger legal provisions in terms of actual safeguards concerning provisions on data privacy such as the types of personal data that need protecting (*see 3.2.1*), legitimate processing that adheres to principles of purpose limitation and proportionality (*see 3.2.3*) and rules on consent (*see 3.2.5*) and the transfer of data to third countries (*see 3.2.6*). The law is assisted by the advisory guidance of the Art29 WP, the European Data Protection Supervisor and national data protection authorities such as the Information Commissioner's Office in the UK (*see 3.2.3.2; 6.4.1*). Nevertheless, further room for improvement would be for the EU to consider the best interests of the child, to provide uniform rules on the age at which children can provide online consent (*see 1.2.3; 4.10.1*), and to regulate the practice of privacy policies with the aim to achieve harmony in EU member states concerning children's use of the internet (*see 1.2.3; 4.10.1*).

The EU supervisory authorities should have adequate funding and properly trained staff to carry out enforcement actions (*see 4.10.4*). EU should empower its supervisory authorities as do the Federal Trade Commission and the California

Attorney General, who play an active role in shaping data privacy law in the region that is applied through enforcement action and followed by organisations in the U.S.

The next section looks at the main findings of Chapters 5 and 6, which carried out a two-part multiple case study of the privacy policies of 10 videogame websites based on 11 criteria for evaluation (*Chapter 5 Table 4*).

8.4. Findings of the videogame multiple case study

Videogame websites collect information from users including children in return for using their services (*see 5.1*). The website will process the information in accordance with the legal requirements of the country of its registration. In its privacy policy, websites should inform users of its data handling practices, which will include determining the type of information collected, what happens to the information that is collected, whether the information is shared with third parties, what if any rights there are for website users to access, correct and/or delete their personal information held by the website etc.¹⁰⁹⁹ The multiple case study in Chapter 5 considered whether the information presented in the privacy policies could easily be accessed, read, understood and consented to by children and their parents.

Chapter 6 analysed the second part of the multiple case study: whether privacy policies complied with governing data privacy law. The analysis was based on the study of 11 criteria to evaluate privacy policies (*Chapter 5 Table 4*). The criteria for evaluation emulated the sequence of data privacy laws regulating data handling practices (*see 5.4*). In summarising the observations, seven key findings of both

¹⁰⁹⁹ Ian J. Turnbull, *Privacy in the Workplace* (CCH Canadian Limited 2009).

chapters will be presented in the following paragraphs, namely the issue of readability with privacy policies; the absence of a governing law that will regulate the terms of the privacy policy; the unclear purpose of privacy frameworks; the extensive collection of personal information from users; the difficulty of the methods to disable/opt out of cookies; the failure to mention the parental consent methods; and the potential for subject access requests to be declined for vague reasons.

According to Aleecia M. McDonald and Lorrie Faith Cranor, 'Studies show privacy policies are hard to read, read infrequently, and do not support rational decision making'¹¹⁰⁰ (see 3.2.5.1). Privacy policies leave a lot to be desired in terms of clarity and ease of comprehension. The research found that most privacy policies across legislatures were updated on 1 January 2017,¹¹⁰¹ (see 5.5.2 & 5.5.2.1) which made changes to the length and wording of the policy (see 5.5.2.1). Despite significant and constant attempts to discover the impetus on the part of the videogame industry for updating the privacy policies, no definitive authoritative source was able to be confirmed.¹¹⁰²

The privacy policies were lengthy and dense documents that expected users to go through the privacy policies of third-party links they clicked on as well (see 5.5.2; 6.2.2, 6.4.1 and 6.6.1). The policies are located at the bottom of the main webpage, lack any distinctive features required under the data privacy laws, (see 5.5.1; 6.2.1, 6.4.1 & 6.6.1) and use complicated and legal jargon. The policies did not stipulate the governing law that regulates the terms of the agreement, leaving users in the dark

¹¹⁰⁰ Aleecia M. McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' <<http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>> accessed 5 February 2018.

¹¹⁰¹ Recently 6 videogame website privacy policies were updated in late 2017 and 2018.

¹¹⁰² Ibid.

about their rights and obligations.¹¹⁰³ The existence of privacy frameworks such as TRUSTe privacy certification and the Privacy Shield Framework may be considered problematic for the user, especially children.¹¹⁰⁴ Websites collected extensive information from users which goes beyond the information required to register for the account such as username and email address (see 5.5.6). The privacy policies infringed the principle of minimality,¹¹⁰⁵ (see 3.2.3.3) and purpose specification (see 3.2.3.2–3.2.3.3; 5.5.6.3).

Another key finding of the study was that the method to opt out of or disable cookies was complicated and difficult to follow,¹¹⁰⁶ there was no method to obtain verifiable parental consent,¹¹⁰⁷ and the methods for data subjects to access their data were not simple and easy to follow.¹¹⁰⁸

The key findings of the comparative legislative analysis between the legislation in the EU, the U.S. and Canada and the multiple case study of 10 videogame website privacy policies have been presented. The study reveals that privacy policies are not designed for children. There is a wide understanding that children should learn and enjoy reading literature. Instead, they are expected to read lengthy, complicated legal documents and follow cumbersome methods to alter their privacy settings. Consent is a core principle of data protection law. But valid consent is difficult to obtain and prove.

¹¹⁰³ Chapter 5 Sections 5.4.1 and 5.5.3; Chapter 6 Sections 6.2.3, 6.4.2 and 6.6.2; Chapter 7 Section 7.6.

¹¹⁰⁴ Chapter 5 Sections 5.5.4 and 5.5.5; Chapter 6 Sections 6.2.4, 6.2.5, 6.4.3, 6.4.4 and 6.6.3.

¹¹⁰⁵ Directive 95/46/EC Article 6(1)(c); Chapter 3 Section 3.2.3.3; EU GDPR 2018 Article 5(1)(c).

¹¹⁰⁶ Chapter 5 Section 5.5.9.1; Chapter 6 Sections 6.2.8, 6.4.7, 6.4.7.1 and 6.6.4.

¹¹⁰⁷ Chapter 1 Section 1.2.4; Chapter 3 Sections 3.2.5.3 and 3.2.5.7; Chapter 4 Sections 4.3.3.2, 4.3.3.3 and 4.10.3; Chapter 5 Section 5.5.10.2; Chapter 6 Sections 6.2.9, 6.4.8 and 6.6.5.

¹¹⁰⁸ Chapter 3 Section 3.2.7; Chapter 5 Section 5.5.11; Chapter 6 Sections 6.2.10, 6.4.9 and 6.6.6.

Despite the difficulties to digital privacy that have resulted from commercial data tracking, industry experts are moving towards informing and empowering data subjects with the right to regulate and monitor their personal data. In the UK, the National Society for the Prevention of Cruelty to Children (NSPCC)¹¹⁰⁹ has partnered with O2¹¹¹⁰ to launch the project 'Keeping Kids Safe Online'.¹¹¹¹ The project runs workshops in schools to help teachers, parents and children to have the right conversations about online safety. The project specifically delivers workshops on protecting against online sexual grooming, abuse, trolling and hacking. There is little information on data tracking techniques and possible commercial exploitation by websites. Similarly, Google introduced an online videogame, titled *Interland: Be Adventure Awesome*,¹¹¹² to improve digital safety knowledge of children. It taught children to distinguish between fake and real online identities/profiles on social media websites, to share information with care, to speak against bullying and to block inappropriate behaviour. However, the game does not educate children on protecting against commercial exploitation. Children are not informed about the importance of reading privacy policies and managing privacy settings, how to respond to targeted advertisements, in-game purchases, requests to taking part in surveys and general interaction in chat rooms and social forums within videogame websites.

¹¹⁰⁹ The NSPCC helps children who have been abused to rebuild their lives, protect those at risk and investigates the ways of preventing abuse from happening in the future NSPCC <<https://www.nspcc.org.uk/>> accessed 2 February 2018.

¹¹¹⁰ O2 is a provider of mobile phones, mobile broadband and sim-only deals. O2 <<https://webcache.googleusercontent.com/search?q=cache:SMtn5342EusJ:https://www.o2.co.uk/+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2018.

¹¹¹¹ NSPCC and O2 <<https://www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership/>> accessed 2 February 2018; Young Ji Lee, Sitwat Langrial and Wu-Chen Su, 'Are Parents Getting It Right? A Survey of Parents' Internet Use for Children's Health Care Information' (2015) 4(2) *Interact J Med Res*.

¹¹¹² *Interland: Be Adventure Awesome* is a free, adventure web-based game that allows kids to learn about digital privacy through game play. 'Interland: Be Internet Awesome' (fwa, June 2017). <<https://thefwa.com/cases/interland-be-internet-awesome>> accessed 9 March 2018.

On the global scene, the Hilton Hotel & Resorts¹¹¹³ brand published a global privacy policy on 14 November 2017¹¹¹⁴ with one of the aims being to clarify rights of individuals in certain foreign jurisdictions. A global privacy policy is an example of good practice where organisations operate in multiple jurisdictions.

It is argued that there is lack of understanding of children's digital privacy rights by regulators. Baroness Beeban Kidron¹¹¹⁵ proposed to introduce new laws to protect children online based on targeted advertising, endless notifications and indiscriminate data gathering practices causing social anxieties and the risk for personal information to be disseminated online.¹¹¹⁶

The UK's prior health secretary, Jeremy Hunt, penned a letter to social media giants including Facebook and Google, stressing that age verification, limits on screen time and cyberbullying should be addressed.¹¹¹⁷ The government is finally taking notice of the importance of children's digital privacy. However, age verification methods are based on the supply of personal information and will always be difficult to prove. Limitation on screen time can have a negative impact on children's use of the internet.

As a comparison, the indoor tobacco smoking ban did result in overall improved health, but it was more effective for those who were already smoking fewer

¹¹¹³ Hilton <<http://www3.hilton.com/en/index.html>> accessed 20 April 2018. Hilton Hotel & Resorts is a global brand of full-service hotels under the Hilton brand.

¹¹¹⁴ Hilton Honors <<http://hiltonhonors3.hilton.com/en/policy/global-privacy-statement/index.html>> accessed 20 April 2018.

¹¹¹⁵ See Footnote 115.

¹¹¹⁶ Anushka Asthana, 'Lords Push for New Regulations to Protect Children Online' *The Guardian* (18 November 2017) <<https://www.theguardian.com/society/2017/nov/18/lords-push-for-children-to-be-protected-against-tech-giants-by-law>> accessed 9 March 2018.

¹¹¹⁷ 'Jeremy Hunt Threatens Social Media with New Child-Protection Laws' (BBC News, 22 April 2018) <<http://www.bbc.co.uk/news/uk-43853678>> accessed 2 May 2018.

cigarettes a day than for heavy smokers.¹¹¹⁸ Screen time limitation will have psychological effects on children depending on how often they use the internet. It is proposed that children and their parents be educated on the importance of digital privacy. Schools should introduce digital privacy as a curriculum so that children can learn to make educated choices early on.

If children are expected to read and consent to the terms of the privacy policy, it is imperative that they understand the consequences in terms of the legal rights and obligations that arise once consent is provided. Based on the notion of informed choices, as well as the findings in Chapters 3 – 6, and best practices from the privacy policies of children’s interactive videogames, (see 7.2 - 7.6) a child-friendly model privacy policy has been drafted (see 7.7).

This is the main contribution to this thesis and to existing literature that addresses children’s digital privacy in online videogame websites (see 7.7). The child-friendly model privacy policy will prove a valuable contribution as it addresses the readability issue by being brief, utilising easy-to-understand language and eliminating difficult-to-follow methods to opt out of data tracking. It also addresses the unreasonable expectation that children should read, understand and consent to lengthy and complicated privacy policies (see 7.7). It takes account of the provisions of the EU

¹¹¹⁸ Daughton M.S. and others, ‘Total Indoor Smoking Ban and Smoker Behavior’ (1992) 21(5) Preventive Medicine; Jennifer McGowan and Lion Shahab, *Psychological Aspects of Tobacco Control* (Oxford University Press July 2017) <<http://psychology.oxfordre.com/view/10.1093/acrefore/9780190236557.001.0001/acrefore-9780190236557-e-126>> accessed 2 May 2017. The use of tobacco is a leading cause of morbidity, making smoking cessation an important health policy. However, a complete ban can have negative effects. Policymakers should understand the personal and interpersonal factors (including social norms, mental health and individuals’ personality factors) responsible for smoking habits.

GDPR 2018 which makes consent an affirmative and positive action and introduces an opt-in and opt-out button for cookies.

Since the child-friendly model privacy policy is for children, it maximises the possibility that they will read and understand it. Consent is not implied, like in other privacy policies, but it is an affirmative and positive action that requires a click to agree to the terms once the document is read. Understanding is guaranteed with the very easy language that dismisses the use of any complicated words or the fuss of additional links providing meaning. Cookie consent is not presented on the homepage that forces users to consent or leave the page. It is embedded within the privacy policy. The governing law is added as a link that contains a short document encompassing the main provisions for both parents and children to understand (*see 7.7 & Annex 1*).

At an industry level, videogame websites can make the necessary amendments and incorporate the child-friendly model privacy policy so that children can conveniently access, read, understand and consent to them. If it is not possible to change the privacy policy, videogame websites directed to children should have an additional privacy notice incorporating the child-friendly model privacy policy. This is also helpful for parents because they will be better informed of the videogame websites' data handling practices their children interact with (*see 1.4*).

Instead of feeling overwhelmed with digital information and a lack of knowledge on privacy protection tools, (*see 2.5.1*) they will feel empowered when exercising their right to provide verifiable consent. This is because they can make conscious decisions about whether they agree with the websites' collection of their children's data, the

governing legislation that regulates the terms of the agreement, the button to disable cookies, whether they can access and/or correct their children's data, and the method they can use to verify consent. If they do not agree with the terms and conditions of the privacy policy, they can withhold consent, which will automatically prevent children from playing the videogame.

8.5. Best practices: Mini-case study

The mini case study of Disney.com, CBeebies (bbc.co.uk/cbeebies), and Harry Potter website(www.warnerbros.co.uk) revealed that industrial practice regarding children's digital privacy rights still demonstrates gaps. Privacy policies are still too long and collect extensive information from users using vague reasons such as 'improving user experience' as a purpose to collect personal data. Methods for parental consent are not specified and third parties are operating on the host website which can collect information belonging to children.

Best practices from the mini-case study revealed that the privacy policy uses easy to understand language, methods to disable cookies are simple with a single swipe of a button, there is a separate children's privacy policy.

The MPP has retrieved such best practices and combined them with the findings from the multiple case study in Chapters 5 and 6 to draft a brief, easy to understand children's privacy policy that treats children as a special class of data subjects.

8.6. Original child-friendly model privacy policy

A key original contribution to this thesis is the child-friendly model videogame privacy policy aimed at children (*Chapter 7*). The aim is that this model policy informs

videogames to post privacy policies that are comprehensive and easy to read and understand for children and their parents.

8.6.1. Key features of the child-friendly model privacy policy: a shorter word length

Key features of the model privacy policy include a shorter word length of 562 words (see 7.7). This is strikingly less than the average 4,000 words in the videogame privacy policies updated on 1 January 2017. The 10 privacy policies also contained links that allowed users to read additional documents, including third-party privacy policies, methods to disable cookies, privacy frameworks etc., which excessively add to the current word length of 4,000 words. The model policy includes a single link that takes the user to the governing law, containing a summary of the main provisions in 246 words. This brings the total word count to 808 words. The Flesch reading score of 100–90 is used as the standard of readability for an 11-year-old or fifth-grade child.

8.6.2. Clearly displayed governing law

The model policy places the governing law at the outset, which can be clicked to view a brief version of the law containing the main provisions in very simple language. Only Disney.com presents the governing law at the outset, in its Children’s Privacy Policy, (see 7.3.1.3) but a link takes the user to the entire COPPA text, which is a legally onerous document to read.

8.6.3. Collection of personal data should respect principles of minimality and informed consent

An important finding in the multiple case study of privacy policies reveal the extensive information collected from children without giving clear and obvious reasons for doing so (*see 5.5.6*). This should not happen because for legitimate processing of personal data, amongst other things, the data subject should provide a clear, informed and unambiguous consent to the processing.¹¹¹⁹ For legitimate processing to occur, users should be informed about the purpose behind the collection, processing and storage of personal data.¹¹²⁰ Additionally, the legitimate processing should follow the principle of minimality.¹¹²¹ The study shows that data subjects are not given the option to provide clear and unambiguous consent. There are four privacy policies that have not been updated after the coming into force of the EU GDPR 2018 (*see 5.5.1*).¹¹²² They still imply consent as soon as the data subject accesses the website or starts to play the game (*see 5.5.6.2*). If the privacy policy is difficult to understand, then consent will not amount to an informed indication of the user's wishes.

The model policy includes five categories of information and the purpose behind collection is dealt with in a separate paragraph. In addition, readers are advised to be careful about sharing their information online and warned of the risks that strangers can view their information publicly.

¹¹¹⁹ Directive 95/46/EC Article 7(a); EU GDPR 2018 Article 4(11).

¹¹²⁰ Directive 95/46/EC Article 6(1)(b) and Recital 28; EU GDPR 2018 Article 5(1)(b).

¹¹²¹ Directive 95/46/EC Article 6(1)(c); EU GDPR 2018 Article 5(1)(c).

¹¹²² Princess Isabella; Heroes of the Storm; Pogo; Prince of Persia.

The model policy acknowledges consent as a positive and informed action on the part of the user. To be an affirmative action, consent is given by clicking a button rather than implied. Users can also exercise an informed choice because the model policy is explained in concise and easy-to-understand terms (see 7.7). For children below a certain age, a verifiable parental consent method has been provided and explained using simple language.

8.6.4. Method to disable cookies is a single click

The model privacy policy avoids the use of links, which expects children to read lengthy, complicated procedures to disable cookies. It does not expect children to refer to their browsers and alter their privacy settings accordingly. Instead, the model policy facilitates by reminding children and their parents about the importance of their privacy settings and the method to disable cookies is a single click.

The model policy avoids using vague reasons to reject subject access requests. The method to send such a request is through an automated message box for the convenience of the user.

In conclusion, the model privacy policy aims to present a website's data handling practice in concise and easy-to-understand terms. It aims to revolutionise the industry of posting lengthy, complicated privacy documents that are rarely read by users, let alone children.

8.7. Limitations of the study

The findings of this study are prone to certain limitations for the following reasons. First, this thesis, to a considerable extent, represents desk-based research that is

largely built on the available literature study. There is plentiful research on the online privacy risks such as cyberbullying,¹¹²³ sexual exploitation,¹¹²⁴ racism,¹¹²⁵ trolling and online harassment.¹¹²⁶ Limited research exists on the commercial exploitation of children when interacting with the online community such as playing videogames¹¹²⁷ (see 1.3). It might be speculated that a lack of research in this area may have caused incoherent and inadequate regulatory measures on the EU, U.S. and Canadian data privacy level. Social scientists could change this situation by means of empirical research because data breaches¹¹²⁸ do not show whether the data belonged to children and evidence of commercial exploitation is even harder to locate.

One other limitation is the child friendly model privacy policy (see section 7.7) was not created in consultation with children. Instead, it was based on findings from the comparative and multiple case study research conducted in Chapters 5 and 6. This thesis studies the data protection and privacy jurisdictions of the EU, the U.S. and Canada. The EU data privacy legislation was selected as it was not practical to study the data privacy laws of each EU member state. Instead, the earlier Directive 95/46/EC and the EU GDPR 2018 which applies in EU domestic members, was studied

¹¹²³ Adina Farrukh, Rebecca Sadwick and John Villasenor, 'Youth Internet Safety: Risks, Responses, and Research Recommendations' (Center for Technology Innovation at Brookings, October 2014) <https://www.brookings.edu/wp-content/uploads/2016/06/Youth-Internet-Safety_v07.pdf> accessed 6 February 2018.

¹¹²⁴ Danielle Deep, *Role of the Internet in the Sexual Exploitation of Children* (ProQuest Dissertations Publishing 2016).

¹¹²⁵ 'Online Abuse Facts and Statistics' (NSPCC) <<https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/facts-statistics/>> accessed 6 February 2018.

¹¹²⁶ 'Ofcom Report on Internet Safety Measures' (Ofcom 12 January 2015) <https://www.ofcom.org.uk/data/assets/pdf_file/0016/31732/Third-internet-safety-report-January-2015.pdf> accessed 6 February 2018.

¹¹²⁷ Grace Chung and Sara M. Grimes, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2005) 30(4) *Canadian Journal of Communication*; Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps' (2017) 26(2) *Information & Communications Technology Law* 146.

¹¹²⁸ 'Hackers Steal Millions of Minecraft Passwords' (BBC News, 29 April 2016) <<http://www.bbc.co.uk/news/technology-36168860>> accessed 27 October 2017.

as a benchmark. Since the study of this thesis began in September 2017, the now repealed EU Directive 95/46/EC forms an integral part of the discussion. It provides insight into the adequacy of data privacy law and website's data gathering practices (privacy policies) to protect children's digital privacy rights before and after the EU GDPR 2018 came into force.

Retrieving a Canadian videogame was another issue (*see 5.3.1.3*) because most games developed and published in Canada were eventually sold off to foreign companies.¹¹²⁹ There is a lack of specific provisions regulating children's digital privacy rights, permitting limited discussion on the subject.

The reason behind the update of videogame privacy policies on 1 January 2017¹¹³⁰ is an unresolved issue (*see 5.5.2.1*). Journal articles and other relevant material have been covered, and the ICO was contacted, but the outstanding question has yet to be determined. It would be interesting to consider what commercial agreements and legal developments might have influenced updates in the privacy policies. Another update of six privacy policies occurred in late 2017 and early 2018 (*see 5.5.1*). It is likely that this update occurred to ensure compliance with the EU GDPR 2018.

¹¹²⁹ Craig Chapple, 'Licence to Thrill: Behind the Scenes at Beenox' (Develop, 23 November 2015) <<https://webcache.googleusercontent.com/search?q=cache:cKGuVtsrh9MJ:https://www.mcvuk.com/development/licence-to-thrill-behind-the-scenes-at-beenox+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 23 January 2017.

¹¹³⁰ *League of Legends; Dota 2; Minecraft; Heroes of the Storm; Pogo; Miniclip; Princess Isabella; Candy Crush Saga; Clash of Clans. Prince of Persia* was updated on 12 January 2016 <<https://legal.ubi.com/privacypolicy/en-US>> accessed 24 January 2017.

8.8. Recommendations for future research

The media and entertainment industry are adopting data mining¹¹³¹ and big data¹¹³² technologies at an unprecedented rate. This should encourage policymakers and academics to carry out wider investigation for the understanding of children's interaction with the digital media and entertainment system. Traditionally, research has been conducted into children's exposure and use of the internet. In more recent times, children have become one of the largest demographic groups to use the internet for a multitude of reasons including playing games, using social media and search engines, entertainment and education-based activities (*see 1.1*). At present, children's engagement with the internet has become personally interactive.

At present, the limited research conducted into children's digital privacy is primarily desk-based, carrying out a literature study of existing material produced by others.¹¹³³ Research should go beyond traditional social science methods and conduct more collaborative and interdisciplinary analysis with experts from different fields such as child psychologists, gaming and social media experts, data privacy experts and law makers. Global Kids Online¹¹³⁴ has identified that available statistics and research literature provides uneven evidence on children's experience of

¹¹³¹ 'Data mining is the process of discovering interesting patterns and knowledge from large amounts of data' Jiawei Han, Micheline Kamber and Jian Pei, *Data mining concepts and techniques* (Elsevier 2012).

¹¹³² Big data refers to the massive volume of structured and unstructured information that is so extensive it is difficult to process using traditional data mining techniques. Big data is classified by three main features: volume refers to the massive information of data; variety refers to the extensive structured and unstructured types of data; and velocity refers to the speed at which the data is processed. Vitthal Yenkar and Mahip Bartere, 'Review on "data mining with big data"' (2014) 3(4) IJCSMC 97.

¹¹³³ Piet Verschuren and H. Doorewaard, *Designing a Research Project* (Eleven International Publishing 2nd revised edition 2010); L. Jasmontaité, 'Children's Online Privacy and Data Protection by Self-Regulation Adopted on the EU Level: A Reality or an Illusion?' (Tilburg University, October 2012).

¹¹³⁴ Global Kids Online works in an international research project that collaborates with UNICEF, the London School of Economics and Political Science (LSE) and the EU Kids Online network to generate cross-national evidence around children's use of the internet. Global Kids Online <<http://globalkidsonline.net/>> accessed 25 April 2018.

internet use.¹¹³⁵ Such information is vital for generating policies relating to children's best interests, welfare, the economy and society.¹¹³⁶ According to Global Kids Online, research requires contributions from academics, governments, civil society and experts that can come together and apply different research tools for comparative findings across countries and contexts.¹¹³⁷ Most importantly, children should be allowed to share their experiences and their voices heard to improve policymakers' understanding of children's rights in the digital age.¹¹³⁸ Research should also consider the ongoing market trends, real-world practices, current and prospective data privacy laws, industrial movements with regard to protecting children's digital privacy etc.¹¹³⁹

8.9. The final message

The main goal of the thesis was to examine whether videogame privacy policies comply with the governing law, and if the governing law and practice of privacy policies remain commensurate with the expectation for children to access, read, understand and consent to privacy policies. Yet, it appears from the summary of the main research findings that, thus far, this is an unattainable objective. This is because the law has established core data protection principles on the digital privacy rights of

¹¹³⁵ Sonia Livingstone, 'A Method for Researching Global Kids Online – Understanding Children's Well-Being and Rights in the Digital Age' (Global Kids Online November 2016) <<http://globalkidsonline.net/>> accessed 25 April 2018.

¹¹³⁶ Ibid.

¹¹³⁷ Global Kids Online research toolkit – quantitative guide <<http://globalkidsonline.net/>> accessed 25 April 2018.

¹¹³⁸ Ibid.

¹¹³⁹ Belinha S. De Abreu and others, *International Handbook of Media Literacy Education* (Routledge 2017); Robinson Meyer, 'Everything We Know about Facebook's Secret Mood Manipulation Experiment' *The Atlantic* (24 June 2014) <<https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>> accessed 2 February 2018; Vindu Goel, 'Facebook Tinkers with User's Emotions in News Feed Experiment, Stirring Outcry' *The New York Times* (29 June 2014) <<https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html>> accessed February 2018.

children but there are gaps that need to be further addressed to ensure children are treated as a special class of data subjects.

The three key findings of this study were the varying ages for consent used in different jurisdictions, the issue with reliability of online consent methods and the identity of the person furnishing consent, and the difficulty with the readability of privacy policies.

The online videogame industry is a borderless world where games registered in one country are conveniently accessed from any other part of the world. Different jurisdictions have varying ages for online consent. Videogame players will be subject to different levels of protection. The UNCRC is ratified by 196 states in the world¹¹⁴⁰ and defines a child as anyone under the age of 18 years.¹¹⁴¹ It is recommended that data privacy legislatures adopt this same standard and require children under 16 years to provide verifiable parental consent.¹¹⁴²

Consent is defined as ‘any freely given specific and informed indication of the data subject’s wishes for their data to be processed’.¹¹⁴³ In the digital environment, children are expected to consent to privacy policies that are lengthy, complicated legal documents.

¹¹⁴⁰ UN Convention on the Rights of the Child Article 1; United Nations treaty collection <https://webcache.googleusercontent.com/search?q=cache:nr6kif9nff4J:https://treaties.un.org/Pages/ViewDetails.aspx%3Fsrc%3DIND%26mtdsg_no%3DIV-11%26chapter%3D4%26lang%3Den+&cd=1&hl=en&ct=clnk&gl=uk> accessed 14 April 2018.

¹¹⁴¹ UNCRC Article 1.

¹¹⁴² This recommendation is compatible with EU GDPR 2018 Article 8(1), which requires children under 16 years to provide consent by the holder of parental responsibility over the child.

¹¹⁴³ Directive 95/46/EC Article 2(h). Consent is further categorised into explicit consent which is given for sensitive data Directive 95/46/EC Article 8(2)(a). Consent is needed to ensure legitimacy of processing as well as transfer of data to third countries that do not possess adequate levels of protection. Directive 95/46/EC Article 26(1)(a).

It is recommended that website operators limit the importance attached with consent as a form of authorisation for data processing. Instead, website operators should rely on data protection principles of minimality,¹¹⁴⁴ (see 3.2.3.3) transparency and purpose specification to ensure that children's digital privacy remains safe (see 1.2.4; 4.10.4; 6.2.9).

We have separate rights for children in different areas. Films are rated based on development stages; children are offered special protection with regards to sexual activity; there are age limits for children to smoke, drink alcohol and drive. Children are also protected in environments where adults smoke, drink and drive. The overriding understanding is that society should have global consensus to act in the best interests of the child.¹¹⁴⁵ It should agree that, owing to a child's vulnerability and level of maturity, they may have a limited capacity to act and understand online interaction. Yet the digital environment does not present this consensus.¹¹⁴⁶

Firstly, it was found that the age at which children can provide consent differs between legislatures, creating different levels of protection.¹¹⁴⁷ Data privacy legislation should treat children as a special class of data subjects that deserve extra protection. Additionally, the industry should agree upon a common age for furnishing consent¹¹⁴⁸ (see 1.2.3; 4.9.1). It was also found that it is difficult to prove an

¹¹⁴⁴ Directive 95/46/EC Article 6(1)(c): the principle of minimality limits data collection to achieve the purpose behind the collection.

¹¹⁴⁵ 'Baroness Beeban Kidron' (The Children's Media Conference)

<<http://www.thechildrensmediaconference.com/profile/baroness-beeban-kidron/>> accessed 20 April 2018.

¹¹⁴⁶ Baroness Beeban Kidron OBE, 'Children and Digital Rights: Regulating Freedoms and Safeguards' (Ials, 17 November 2017) <<http://ials.sas.ac.uk/digital/videos/children-and-digital-rights-regulating-freedoms-and-safeguards>> accessed 24 January 2018.

¹¹⁴⁷ EU GDPR 2018 Article 8(1).

¹¹⁴⁸ 'Child' should be defined as anyone under the age of 18 years. UN Convention on the Rights of the Child, Article 1; Delaware Online Privacy Protection Act Section 1201C(6).

identifiable consent. Legal tradition dictates that consent is an informed, positive and unambiguous action when the user has been given all the relevant information regarding the possible consequences of giving consent.¹¹⁴⁹ While such a strict requirement is perfectly plausible, it is excessively hard to prove if privacy policies imply consent by simply entering the website and if children and/or their parents have to read lengthy, dense and complicated legal documents. Instead, reliance may be had on principles of minimality and purpose specification to ensure children's digital privacy remains safe and secure.

The two-part multiple case study revealed that the privacy policies are not compatible with the reading abilities of children. Furthermore, it was found that the structure and format of the privacy policies create an issue of readability because they are complicated, dense and lengthy legal documents (*see 2.5.2*). The privacy policies had an average word length of 4,000 words, which constitutes 8 A4 pages. The privacy policies use difficult words and do not follow a standard for readability. Extensive information is collected from children. Vague reasons such as 'improving user experience' are given to justify the collection. In addition, various forms of tracking technologies are used and methods to disable cookies are difficult to follow, which deters users from doing anything about their privacy settings.

The updated privacy policies contain a separate children's privacy policy; are framed in simpler terms explaining the functioning of different cookies operating on the website. However, this has resulted in lengthy privacy policies, some policies are still

¹¹⁴⁹ Dan Jerker B. Svantesson, *Private International Law and the Internet* (Kluwer Law International 2007).

employing complicated methods to opt-out of cookies, and they lack a parental consent mechanism.

It is recommended that laws should require privacy policies to be located at the top of the homepage to be easily discernible; they should be brief and use a standard of readability that coincides with the reading level of an 11-year-old. Data privacy laws should provide guidance on the kinds of information that can be collected, explaining the reasons for doing so, and methods to disable cookies should be simple, preferably a single click for the benefit of children.

An issue was encountered with the privacy policy failing to mention the specific governing data privacy law (contained in the terms and conditions) that regulates the terms of the privacy policies. Users will be unaware of the rights and obligations they are entitled to. To keep children and/or parents informed of their legal obligations, each privacy policy should contain a link that can be clicked on to access a simple, brief legal document containing the main provisions of the law.

The child-friendly model privacy policy in this thesis is one of the first steps towards ensuring that children are better equipped with the required digital skills to safely interact with the online community. UK Culture Secretary Matt Hancock states that there is 'genuine concern' about the time children spend online and providing false ages to register onto websites.¹¹⁵⁰ The government is proposing that companies should ensure users are over 13 years old. The objective of the government should be to make children digitally literate and require websites to post child-friendly

¹¹⁵⁰ 'Have Your Say: Should We Restrict Children's Social Media Use?' (Sky News, 10 March 2018) <<https://news.sky.com/story/have-your-say-should-we-restrict-childrens-social-media-use-11283498>> accessed 10 March 2018.

privacy policies that will encourage them to read and understand data handling practices. When children are informed, they can make better and more prudent choices online.

Annex 1

Children's Online Privacy Protection Act¹¹⁵¹

To protect the online data collection of children aged 13 and under on the internet, United States officials have passed the Children's Online Privacy Protection Act (COPPA) in 2000. Under COPPA, websites should meet certain privacy policy requirements, limits on data collection from users and placing verifiable consent mechanisms within the privacy policy.

Directly below, you will find a summary of the main principles of COPPA –

COPPA APPLIES TO –

Anyone that operates an online service or commercial website that attracts children under 13 years.¹¹⁵²

UNDER COPPA, A WEBSITE SHOULD –

Post a prominent and clearly labelled link to a privacy policy on the homepage of the Web site¹¹⁵³ of what information it collects from children.¹¹⁵⁴

UNDER COPPA, THE PRIVACY POLICY SHOULD PROVIDE-

The name and address of operators of the website.¹¹⁵⁵

The kind of information being collected from users.¹¹⁵⁶

How the operator will use this information.¹¹⁵⁷

If information is shared with third parties, the identity of third parties and how they will use the information.¹¹⁵⁸

¹¹⁵¹ Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

¹¹⁵² Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505; 16 CFR § 312.2.

¹¹⁵³ 16 CFR § 312.4.

¹¹⁵⁴ 16 CFR § 312.3 (a) & 312.4.

¹¹⁵⁵ 16 CFR § 312.4 (d)(1).

¹¹⁵⁶ 16 CFR 312.6 (a)(1).

¹¹⁵⁷ 16 CFR 312.6 (d)(2).

¹¹⁵⁸ COPPA 16 CFR 312.4 (d)(1).

Notice to parents about the parental consent mechanism whereby parents can consent to the collection of their children's information by operator.¹¹⁵⁹

Parents' right to review their children's information and make requests to change/delete it.¹¹⁶⁰

COPPA APPLIES TO WEBSITES THAT COLLECT PERSONAL INFORMATION FROM CHILDREN SUCH AS THEIR –

Full name.¹¹⁶¹

Home address.¹¹⁶²

Email address.¹¹⁶³

Telephone number.¹¹⁶⁴

COPPA will also apply to digital information that is collected through tracking technologies (such as cookies) when it is attached to personally identifying information.¹¹⁶⁵

¹¹⁵⁹ 16 CFR § 312.5 (a).

¹¹⁶⁰ 16 CFR 312.6 (d)(3).

¹¹⁶¹ 16 CFR § 312.2 (1)

¹¹⁶² § 312.2 (2).

¹¹⁶³ § 312.2 (3).

¹¹⁶⁴ § 312.2 (5).

¹¹⁶⁵ § 312.2 (7).

Annex 2

Text of EU General Data Protection Regulation 2018 ARTICLES 5, 6, 7, 12, 13 & 15

CHAPTER II **Principles**

Article 5

Principles relating to processing of personal data

1. Personal data shall be:
 - (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
 - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

- (a) Union law; or
- (b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- (d) the possible consequences of the intended further processing for data subjects;
- (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2
Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- (d) the right to lodge a complaint with a supervisory authority;
 - (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
 - (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
- (a) the purposes of the processing;
 - (b) the categories of personal data concerned;
 - (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (f) the right to lodge a complaint with a supervisory authority;

- (g) where the personal data are not collected from the data subject, any available information as to their source;
 - (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
 4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

BIBLIOGRAPHY

Books

Allen A, *Unpopular Privacy: What Must We Hide* (Oxford University Press 2011)

Bennett CJ and others, *Transparent Lives: Surveillance in Canada* (Athabasca University Press 2014)

Beyleveld D and Brownsword R, *Consent in the Law* (Bloomsbury Publishing 2007)

Brown G, *The Universal Declaration of Human Rights in the 21st Century* (Open Book Publishers 2016)

Bygrave LA, *Data Protection Law* (Wolters Kluwer Law & Business 2002)

Clarke MJ, *Transmedia Television: New Trends in Network Serial Production* (Bloomsbury Publishing USA 2012)

De Abreu, Belinha S. and others, *International Handbook of Media Literacy Education* (Routledge, 2017)

Deep D, *Role of the Internet in the Sexual Exploitation of Children* (ProQuest Dissertations Publishing 2016)

Gorunescu F, *Data Mining: Concepts, Models and Techniques* (Springer Science & Business Media 2011)

Gratton E, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (CCH Canadian Limited 2003)

Guagnin D, Hempel L and Ilten C, 'Bridging the Gap: We Need to Get Together' in *Managing Privacy through Accountability* (Springer 2012)

Habermas J, *The Structural Transformation of the Public Sphere* (MIT Press 1991)

Han J, Pei J and Kamber M, *Data Mining: Concepts and Techniques* (Elsevier 2011)

Harris D and O'Boyle M, *Bates, and Carla Buckley* (2009)

Keynes E, *Liberty, Property, and Privacy: Toward a Jurisprudence of Substantive Due Process* (Penn State Press 2010)

Klosek J, *Data Privacy in the Information Age* (Greenwood Publishing Group 2000)

Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013)

Kozolanka K, *Publicity and the Canadian State: Critical Communications Perspectives* (University of Toronto Press 2014)

Lambert P, *A User's Guide to Data Protection* (Bloomsbury Publishing 2016)

Lambrinoudakis C and Gabillon A, *Risks and Security of Internet and Systems* (Springer 2016)

Lott J, Schall D and Peters K, *ActionScript 3.0 Cookbook: Solutions for Flash Platform and Flex Application Developers* (O'Reilly Media, Inc. 2006)

McDougall B, *Privacy* (West's Encyclopedia of American Law 2005)

Marcella AJ and Stucki C, *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (John Wiley & Sons 2003)

Mawere M, *The Political Economy of Poverty, Vulnerability and Disaster Risk Management: Building Bridges of Resilience, Entrepreneurshi* (Langaa RPCIG 2017)

Miller AR, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press 1971)

Murray A, *Information Technology Law: The Law and Society* (Oxford University Press 2013)

Brian O' Neill, 'Internet Policies: Online Child Protection and Empowerment in a Global Context' (London: Routledge 2013)

Peers S and others, *The EU Charter of Fundamental Rights: A Commentary* (Bloomsbury Publishing 2014)

Perritt HH, *Law and the Information Superhighway* (Aspen Publishers Online 2001)

Price ME, Verhulst S and Morgan L, *Routledge Handbook of Media Law* (Routledge 2013)

Rao HR and Upadhyaya S, *Information Assurance, Security and Privacy Services* (Emerald Group Publishing 2009)

Sheehan KB, *Controversies in Contemporary Advertising* (Sage Publications 2013)

Solove D, *Understanding Privacy* (Harvard University Press 2008)

Svantesson, DJB., *Private International Law and the Internet* (Kluwer Law International 2007)

Thomas R and Walport M, *Date Sharing Review* (Ministry of Justice 2008)

Turnbull IJ, *Privacy in the Workplace* (CCH Canadian Limited 2009)

Tzanou M, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Bloomsbury Publishing 2017)

U.S. Congress, Office of Technology Assessment, *Federal Information Technology: Electronic Record Systems and Individual Privacy, OTA – CIT – 296* (US Government Printing Office 1986)

Van der Hof S, Van den Berg B and Schermer B, *Minding Minors Wandering the Web: Regulating Online Child Safety* (Springer 2014)

Verschuren P and Doorewaard H, *Designing a Research Project* (2nd revised ed., Eleven International Publishing 2010)

Wang J, *Data Mining: Opportunities and Challenges* (IGI Global 2003)

Wright D and Kreissl R, *Surveillance in Europe* (Routledge 2014)

Yin RK, *Case Study Research: Design and Methods*. 1994 (Sage 1994)

Journal articles

Bailey J, 'Systematic Government Access to Private-Sector Data in Canada' (2012) 2(4) International Data Privacy Law 207

[Balogh](#), K et al. 'Risk-taking and decision-making in youth: relationships to addiction vulnerability [2013] [J Behav Addict](#) 12(1)

Barnes SB, 'A Privacy Paradox: Social Networking in the United States' (2006) 11(9)

Bélanger F and Crossler RE, 'Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems' (2011) 35(4) MIS Quarterly 1017

Bessant J, 'Hard Wired for Risk: Neurological Science, 'the Adolescent Brain' and Developmental Theory' (2008) 11(3) Journal of Youth Studies 347

Beyleveld D and Townend DMR, 'When Is Personal Data Rendered Anonymous? Interpreting Recital 26 of Directive 95/46/EC' (2004) 6(2) Medical Law International 73

Borgesius FZ, 'Behavioral Targeting: A European Legal Perspective' (2013) 11(1) IEEE Security & Privacy 82

Brockdorff N and Appleby-Arnold S, 'What Consumers Think' (2013) 7 EU CONSENT Project, Workpackages

Cannataci JA and Bonnici JPM, 'The End of the Purpose-Specification Principle in Data Protection?' (2010) 24(1) International Review of Law, Computers & Technology 101

Cave, Emma, 'Adolescent consent and confidentiality in the UK.' [2009] European journal of health law., 16 (4) Chung G and Grimes SM, 'Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games' (2006) 30(4) Canadian Journal of Communication

Clifford D, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster-Tracking the Crumbs of Online User Behavior' (2014) 5 J Intell Prop Info Tech & Elec Com L 194

Clouse GR, 'Constitutional Right to Withhold Private Information' (1982) 77 Nw UL Rev 536

Conroy S and others, 'Drug Trials in Children: Problems and the Way Forward' (2000) 49(2) Br J Clin Pharmacol 93

Cranor LF, 'Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice' (2012) 10 J on Telecomm & High Tech L 273

Curren L and Kaye J, 'Revoking Consent: A 'Blind Spot' in Data Protection Law?' (2010) 26(3) Computer Law & Security Review 273

Danagher L, 'An Assessment of the Draft Data Protection Regulation: Does It Effectively Protect Data?' (2012) 3(3) European Journal of Law and Technology

Daughton MS and others, 'Total Indoor Smoking Ban and Smoker Behavior' (1992) 21(5) Preventive Medicine

Eisenhardt K and Graebner M, 'Theory Building from Cases: Opportunities and Challenges' [2007] 50(1) Academy of Management Journal

Federal Trade Commission, 'Children's Online Privacy Protection Rule' (1999) 64(212) Fed Regist 59887

Grassel E and Schirmer B, 'The Use of Volunteers to Support Family Carers of Dementia Patients: Results of a Prospective Longitudinal Study Investigating

Expectations towards and Experience with Training and Professional Support' (2006) 39(3) Z Gerontol Geriatr 217

Hope A, 'Risk Taking, Boundary Performance and Intentional School Internet "Misuse"' (2007) 28(1) Discourse: Studies in the Cultural Politics of Education 87

Imperiali R, 'The Data Protection Compliance Program' (2012) 7 J Int'l Com L & Tech 285

Jasmontaitė L, 'Children's Online Privacy and Data Protection by Self-Regulation Adopted on the EU Level: A Reality or an Illusion?' (2012)

Jasmontaite L, and De Hert P, 'The EU, Children under 13 years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet' (2014) 5(1) International Data Privacy Law 20

Jolls C and Sunstein CR, 'Debiasing through Law' (2006) 35(1) The Journal of Legal Studies 199

Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250

Lovell GI, 'Justice Excused: The Deployment of Law in Everyday Political Encounters' (2006) 40(2) Law & Society Review 283

Lupton D and Williamson B, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) 19(5) New Media & Society 780

Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information & Communications Technology Law 146

Marmor A, 'What Is the Right to Privacy?' (2015) 43(1) Philosophy & Public Affairs 3.

McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies' (2008) 4 ISJLP 543

Nyshadham EA, 'Privacy Policies of Air Travel Web Sites: A Survey and Analysis' (2000) 6(3) Journal of Air Transport Management 143

O'Keeffe GS, Clarke-Pearson K and Council on Communications and Media, 'The Impact of Social Media on Children, Adolescents, and Families' (2011) 127(4) Pediatrics 800

Pechmann C and others, 'Impulsive and Self-Conscious: Adolescents' Vulnerability to Advertising and Promotion' (2005) 24(2) Journal of Public Policy & Marketing 202

Proust O and Bartoli E, 'Binding Corporate Rules: A Global Solution for International Data Transfers' (2012) 2(1) International Data Privacy Law 35

Riccardi JL, 'The German Federal Data Protection Act of 1977: Protecting the Right to Privacy' (1983) 6 BC Int'l & Comp L Rev 243

Schermer BW, Custers B and van der Hof S, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics and Information Technology 171

Singh DK and Swaroop V, 'Data Security and Privacy in Data Mining: Research Issues & Preparation' (2013) 4(2) International Journal of Computer Trends and Technology 194

Sipior JC, Ward BT and Mendoza RA, 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons' (2011) 10(1) *Journal of Internet Commerce* 1

Stultiens, L., T. Goffin, P. Borry, K. Dierickx, H. Nys, 'Minors and Informed Consent: A Comparative Approach' *European Journal of Health Law*, 14 (2007)

Szoka BM and Thierer AD, 'COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech' (2009)

Taylor S and Berridge V, 'Medicinal Plants and Malaria: An Historical Case Study of Research at the London School of Hygiene and Tropical Medicine in the Twentieth Century' (2006) 100(8) *Trans R Soc Trop Med Hyg* 707

Taylor M and others, 'When Can the Child Speak for Herself? The Limits of Parental Consent in Data Protection Law for Health Research' (2017) 1–23

Thomson JJ, 'The Right to Privacy' (1975) *Philosophy & Public Affairs* 295

Tracol X, 'Back to Basics: The European Court of Justice Further Defined the Concept of Personal Data and the Scope of the Right of Data Subjects to Access It' (2015) 31(1) *Computer Law & Security Review* 112

Turow J, 'Privacy Policies on Children's Websites: Do They Play by the Rules?' (2001)

Van der Sloot B, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 307

Warmund J, 'Can COPPA Work—An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act' (2000) 11 *Fordham Intell Prop Media & Ent LJ* 189

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4(5) Harv Law Rev 193

Watkins D and others, 'Exploring Children's Understanding of Law in their Everyday Lives' (2018) 38(1) Legal Studies

Whitman JQ, 'The Two Western Cultures of Privacy: Dignity versus liberty' (2003) 113 Yale LJ 1151

Williams CA and Perkins R, 'Consent Issues for Children: A Law unto Themselves?' (2011) 11(3) Continuing Education in Anaesthesia, Critical Care & Pain 99

Yenkar V and Bartere M, 'Review on "Data Mining with Big Data"' (2014) 3(4) International Journal of Computer Science and Mobile Computing 97

Zweigert K and Kötz H, 'Critical Evaluation in Comparative Law' (1973) 5 Adel L Rev 343

Websites

'#339: Project No. P104503; 16 C.F.R. Part 312; Public Comment(s) on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act (COPPA) Through the Children's Online Privacy Protection Rule (COPPA Rule)' (Federal Trade Commission, 15 December 2011) <<https://www.ftc.gov/policy/public-comments/2013/08/initiative-339>> accessed 22 February 2017

<<http://supercell.com/en/parents/>> accessed 18 May 2018

<<http://constitutionus.com/>> accessed 20 June 2016

<http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en> accessed 12 April 2017

<<http://euw.leagueoflegends.com/>> accessed 2 January 2017

<<http://games.disney.co.uk/>> accessed 27 October 2017

<<http://pixelkin.org/games/dota-2/>> accessed 1 January 2017

<<http://store.steampowered.com/app/570/>> accessed 1 January 2017

<<http://supercell.com/en/games/clashofclans/>> accessed 2 January 2017

<<http://us.battle.net/heroes/en/>> accessed 2 January 2017

<<http://www.everybodyplays.co.uk/review/Princess-Isabella-A-Witchs-Curse-Review/343>> accessed 1 January 2017

<http://www.fashionfantasygame.com/>> accessed 17 November 2017

<http://www.iwin.com/games/princess-isabella--a-witchs-curse>> accessed 1 January 2017

<http://www.lawsociety.org.uk/news/stories/article-29-working-party-new-gdpr-guidance-notes/>> accessed 24 January 2018

<http://www.miniclip.com/games/en/>> accessed 2 January 2017

<http://www.nordicity.com/media/20151210faaebhea.pdf>> accessed 23 January 2017

<http://www.oecd.org/about/>> accessed 4 April 2018

<http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm>> accessed 9 December 2017

<http://www.pogo.com/>> accessed 3 January 2017

<http://www.ratemyprofessors.com/ShowRatings.jsp?tid=433413>> accessed 8 December 2017

<https://www.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf> accessed 21 May 2018

<https://breachlevelindex.com/>> accessed 17 November 2017

<<https://en.gamigo.com/>> accessed 17 November 2017

<[https://en.wikipedia.org/wiki/Cortana_\(software\)](https://en.wikipedia.org/wiki/Cortana_(software))> accessed 9 October 2016

<https://en.wikipedia.org/wiki/Massively_multiplayer_online_role-playing_game>
accessed 17 November 2017

'A Loophole in Data Processing' (Bits of Freedom, 11 December 2012)
<https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf> accessed 10 May 2016

<<https://floridaactioncommittee.org/question/internet-identifier-exactly-required-registered/>> accessed 10 December 2017

<<https://king.com/game/candycrush>> accessed 3 January 2017

<<https://legal.ubi.com/privacypolicy/en-US>> accessed 11 December 2017

<<https://legal.ubi.com/privacypolicy/en-US>> accessed 24 January 2017

<<https://minecraft.net/>> accessed 3 December 2017

<<https://minecraft.net/en-us/>> accessed 3 January 2017

<<https://www.aclu.org/united-states-bill-rights-first-10-amendments-constitution>>
accessed 20 June 2016

<https://www.commonsemmedia.org/app-reviews/candy-crush-saga>> accessed 3
January 2017

<https://www.commonsemmedia.org/app-reviews/clash-of-clans>> accessed 2
January 2017

<https://www.commonsemmedia.org/app-reviews/pogo-games>> accessed 3
January 2017

<https://www.commonsemmedia.org/game-reviews/heroes-of-the-storm>>
accessed 2 January 2017

<https://www.commonsemmedia.org/game-reviews/league-of-legends>> accessed
2 January 2017

<https://www.commonsemmedia.org/game-reviews/minecraft>> accessed 2
January 2017

<https://www.commonsemmedia.org/game-reviews/prince-of-persia-the-forgotten-sands>> accessed 2 January 2017

<https://www.commonsemmedia.org/website-reviews/miniclip>> accessed 2
January 2017

<https://www.cookie-law.org/blog/2016/5/13/the-gdpr,-cookie-consent-and-customer-centric-privacy/>> accessed 21 February 2018

<https://www.greenbook.org/company/Lansdowne-Market-Research>> accessed 18
November 2015

<<https://www.techopedia.com/definition/3952/sandbox-gaming>> accessed 3
December 2017

<<https://www.trustarc.com/privacy-certification-standards/>> accessed 17
November 2015

<<https://www.trustarc.com/privacy-certification-standards/>> accessed 28 March
2017

<<https://www.ubisoft.com/en-US/game/prince-of-persia/>> accessed 2 January 2017

<[Proquest Central](#)> accessed 17 May 2016

'2010 Data Protection in European Union: the role of National Data Protection
Authorities' (Europa) <<http://fra.Europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities>> accessed 24 March 2016

'50 countries including Albania, Belgium, Denmark, Germany, France, Italy,
Switzerland and United Kingdom' <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures>> accessed 9 December 2017

'7 Ways to Stay Safe when Using ATMs' (moneyways.co.uk 2015)
<<http://moneyfacts.co.uk/guides/credit-cards/7-ways-to-stay-safe-when-using-atms/>> accessed 25 March 2016

'81/679/EEC: Commission Recommendation of 29 July 1981 Relating to the Council
of Europe Convention for the Protection of Individuals with Regard to Automatic
Processing of Personal Data' (Europa)
<<https://publications.Europa.eu/en/publication-detail/-/publication/d664d1d0-832e-4341-a1bf-7af18d09d9b5/language-en>> accessed 7 April 2016

'88% of Parents Concerned about What Children Can Access Online, Reveals Survey' (ESET)

<<https://webcache.googleusercontent.com/search?q=cache:sgpFi98w6B0J:https://www.eset.com/int/about/newsroom/press-releases/announcements/88-of-parents-concerned-about-what-children-can-access-online-reveals-survey/+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 10 February 2018

<www.disney.com/> accessed 27 October 2017

Abbott A, 'The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?' (The Heritage Foundation, 10 September 2014) <<https://webcache.googleusercontent.com/search?q=cache:c2vWth7rOlsJ:https://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 27 June 2016

'About Statista Inc.' (Statista) <<https://www.statista.com/aboutus/>> accessed 21 February 2017

Adams K, 'Simplifying Governing-Law Provisions, Part 2' (Adams, 13 July 2015) <<http://www.adamsdrafting.com/simplifying-governing-law-provisions-part-2-renvoi/>> accessed 7 March 2017

'ADI Holiday 2015 Report' <<https://webcache.googleusercontent.com/search?q=cache:Hw5r6lsDf2cJ:https://landing.adobe.com/en/na/solutions/digital-index/246230-2015-holiday-shopping-infographic/index.html+&cd=2&hl=en&ct=clnk&gl=uk>> accessed 7 February 2018

'Adolescence' <<https://www.psychologytoday.com/basics/adolescence>> accessed 3 December 2017

'After Brexit: Britain's Future' (Chatham House)
<https://www.chathamhouse.org/research/regions/europe/UK/after-brexit-britain-future?page=1#fragment-0> accessed 16 May 2017

Ahmed K, 'Talk Talk Hack Cost upto £35 M' (BBC News, 11 November 2015)
<<http://webcache.googleusercontent.com/search?q=cache:QyVbhKWW5nwJ:www.bbc.co.uk/news/uk-34784980+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 18 November 2015

Akkad O, 'Canadian's Internet Usage Nearly Double the Worldwide Average' *The Globe and the Mail* (8 March 2011)
<<http://www.theglobeandmail.com/technology/tech-news/canadians-internet-usage-nearly-double-the-worldwide-average/article569916/>> accessed 2 January 2017

'An Introduction to Subject Access Rights' (TaylorWessing, November 2013)
<https://www.taylorwessing.com/globaldatahub/article_intro_sar.html> accessed 25 October 2016

Alexander J, '10 Best Canadian-Made Video Games' *Toronto Sun* (21 August 2013)
<<http://torontosun.com/2013/08/21/10-best-canadian-made-video-games/wcm/0b267bf8-fe60-4639-8b19-8c8c6e600c54>> accessed 21 February 2017

Angwin J and McGinty T, 'Sites Feed Personal Details to New Tracking Industry' *The Wall Street Journal* (30 July 2010)
<<https://www.wsj.com/articles/SB10001424052748703977004575393173432219064>> accessed 18 March 2017

Article 29 EU Data Protection Working Party, 'Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority' (Europa, 13 December 2016)
<[file:///C:/Users/User%201/Downloads/wp244_rev01_enpdf%20\(1\).pdf](file:///C:/Users/User%201/Downloads/wp244_rev01_enpdf%20(1).pdf)> accessed 4 April 2018

Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (Europa, 11 April 2018) [file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20\(1\).pdf](file:///C:/Users/zarak/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20180413_Article29WPTransparencyGuidelinespdf%20(1).pdf) accessed 20 May 2018

Article 29 EU Data Protection Working Party, 'Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision' (Europa, 13 April 2016) <<http://www.pdpjournals.com/docs/88536.pdf>> accessed 14 March 2017

Article 29 EU Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (Europa, 2 April 2013) <http://ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 1 April 2017

Article 29 EU Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (Europa, 9 April 2014) <http://www.dataprotection.ro/servlet/ViewDocument?id=1086> accessed 2 April 2017

Article 29 EU Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (Europa, 9 April 2014) <http://ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 10 May 2016

Article 29 EU Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (Europa, 13 July 2011) <<http://webcache.googleusercontent.com/search?q=cache:fTGjFLcJhgJ:www.pdpjournals.com/docs/88081.pdf+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 14 May 2016

Article 29 EU Data Protection Working Party, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' <<http://194.242.234.211/documents/10160/10704/1619292>> accessed 14 April 2018

Article 29 EU Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (Europa, 2007) <<https://webcache.googleusercontent.com/search?q=cache:hk6F0jzjTOUJ:https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2016/05/19/ek-bijlage-2-definitie-anonieme-gegevens-algemene-verordening-gegevensbescherming/ek-bijlage-2-definitie-anonieme-gegevens-algemene-verordening-gegevensbescherming.pdf+&cd=2&hl=en&ct=clnk&gl=uk>> accessed 6 December 2015

Article 29 EU Data Protection Working Party, 'Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (Europa, 18 February 2008) <<http://www.dataprotection.ro/servlet/ViewDocument?id=358>> accessed 22 April 2017

Article 29 EU Data Protection Working Party, 'Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (Europa, 2005) <www.pdpjournals.com/docs/88080> accessed 16 January 2016

Article 29 EU Data Protection Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records' (Europa) <<http://webcache.googleusercontent.com/search?q=cache:zdDsAaTVdn4J:194.242.234.211/documents/10160/10704/1386451+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 31 March 2017

Article 29 EU Data Protection Working Party, 2010 Opinion 1/2010 on the Concepts of 'Controller' and 'Processor' (Europa) <<http://webcache.googleusercontent.com/search?q=cache:l32kmgLH1xYJ:www.pdpjournals.com/docs/88016.pdf+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 11 December 2015

Ashford, A, 'Involving children in decision making' (Commissioner for Children Tasmania) <<https://www.childcomm.tas.gov.au/wp-content/uploads/2015/06/Guide-to-making-decisions-booklet.pdf>> accessed 1 December 2018

Ashford, W 'Only 5% of charities are ready for GDPR , survey shows' (Computerweekly.com 27 April 2018) <<https://webcache.googleusercontent.com/search?q=cache:ePbvWrmxVAJ:https://www.computerweekly.com/news/252440101/Only-5-of-charities-are-ready-for-GDPR-survey-shows+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 17 June 2018

'Assessing Children's Understanding of Law through Digital Gaming' (University of Leicester, 4 July 2014) <<https://www2.le.ac.uk/departments/law/news-events/law-news/assessing-children2019s-understanding-of-law-through-digital-gaming>> accessed 30 March 2018

Asthana A, 'Lords Push for New Regulations to Protect Children Online' *The Guardian* (18 November 2017) <<https://www.theguardian.com/society/2017/nov/18/lords-push-for-children-to-be-protected-against-tech-giants-by-law>> accessed 14 January 2018

Ayenson M and others, 'Flash Cookies and Privacy II: Now with HTML5 and ET AG Respawning' (10 August 2009) <https://webcache.googleusercontent.com/search?q=cache:4X55IK8ry_UJ:https://pdfs.semanticscholar.org/42cf/18892910afd15b0d6872f16384a7bb6cf915.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed 18 March 2017

Baker M, 'The Teacher's Need to Know versus the Student's Right to Privacy' <https://webcache.googleusercontent.com/search?q=cache:jKEQKYMJnOAJ:https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015-sac/gordon_baker_mary.pdf+&cd=2&hl=en&ct=clnk&gl=uk> accessed 8 February 2018

Bakos Y, Marotta-Wurgler F. and Tossen D, 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' (Jstor, 2014) <<https://webcache.googleusercontent.com/search?q=cache:HELW1FvT1i0J:https://www.journals.uchicago.edu/doi/abs/10.1086/674424+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 15 May 2016

Bambach M, 'Canada's Video-Game Industry Ranks No. 3 Worldwide' <<https://www.theglobeandmail.com/report-on-business/small-business/sb-managing/canadas-video-game-industry-ranks-no-3-worldwide/article9875545/>> accessed 30 December 2017

Barnes J, 'Internet Users' Privacy Concerns May Mean Cookies Start to Crumble' *The Guardian* (2013) <<http://www.theguardian.com/technology/blog/2013/may/24/internet-privacy-cookies-firefox>> accessed 27 January 2016

Barnes S, 'A Privacy Paradox: Social Networking in the United States' [2006] *First Monday* 11(9) <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312>> accessed 2 July 2016

Baroness Kidron B OBE, 'Children and Digital Rights: Regulating Freedoms and Safeguards' (Ials, 17 November 2017) <<http://ials.sas.ac.uk/digital/videos/children-and-digital-rights-regulating-freedoms-and-safeguards>> accessed 24 January 2018

Beaumont R, 'Cookie Law Reform in 2016' (Optanon Privacy Matters, 2016) <<https://www.cookie-law.org/blog/2015/2/10/cookie-law-reform-in-2016/>> accessed 30 January 2016

Big Fish Games, Inc., 'Privacy Policy' <<http://www.bigfishgames.com/company/privacy.html>> accessed 16 March 2017

Big Fish, 'Terms of Use' <<http://www.bigfishgames.com/company/terms.html>> accessed 20 March 2017

Birnhack M, 'Soft Legal Globalisation: The role of the EU Data Protection Directive in the Emerging Global Data Protection Regime' (2008) <<http://www.tau.ac.il/law/minerva2/Birnhack.pdf>> accessed 5 January 2016

Blizzard Privacy Policy <<http://eu.blizzard.com/en-gb/company/about/privacy.html>> accessed 15 March 2017

Bonomelli M, 'Wholly-Owned Subsidiaries: Same Same but Different' (Lexology, 8 April 2014) <<https://www.lexology.com/library/detail.aspx?g=90cc6c72-de1a-4ba7-91d0-7cd7a798c5ed>> accessed 23 January 2017

Brien C, 'Facebook Highlights the Rising Power of Europe's Gaming Industry' (VB, 11 June 2015) <<http://venturebeat.com/2015/06/11/facebook-highlights-the-rising-power-of-europes-game-industry/>> accessed 6 February 2017

Brown M, 'Public Awareness Survey 2008' (Landsdowne Market Research, 2008) <<https://www.dataprotection.ie/documents/trainingandawarenes/PAS08.pdf>> accessed 18 November 2015

'Case Studies in Education' (SRI International) <<https://www.sri.com/research-development/case-studies-education>> accessed 18 January 2017

CBeebies <<https://www.bbc.co.uk/cbeebies>> accessed 30 May 2017

CEOP, 'CEOP: Child Exploitation & Online Protection Centre – internet safety' (NCA) <<https://ceop.police.uk/>> accessed 15 May 2016

Chapple C, 'Licence to Thrill: Behind the Scenes at Beenox' (Develop, 23 November 2015)

<<https://webcache.googleusercontent.com/search?q=cache:cKGuVtsrh9MJ:https://www.mcvuk.com/development/licence-to-thrill-behind-the-scenes-at-beenox+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 23 January 2017

Chapter B.53 (Australian Government) <<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#consent>> accessed 23 January 2018

Children and Online Privacy Survey (The I in Online, 2011) <http://www.chis.org.uk/file_download/49> accessed 17 November 2017

Children and Parents: Media Use and Attitudes Report 2016' (Ofcom, 2016) <<https://www.ofcom.org.uk/research-and-data/media-literacy-research/children/children-parents-nov16>> accessed 24 December 2016

Children's Commissioner, 'Growing Up Digital' (The Children's Commissioner's Office) <<https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/>> accessed 13 January 2018

Children's Data Protection and Parental Consent (Advertising Education Forum, October 2013) <<http://www.aeforum.org/gallery/5248813.pdf>> accessed 22 April 2017

Child employment(gov.uk) < <https://www.gov.uk/child-employment>> accessed 23 November 2018

Children: general (Advertising Standards Authority 17 July 2018) < <https://www.asa.org.uk/advice-online/children-general.html>> accessed 1/12/2018

Children's Online Privacy Protection Rule: A six-Step Compliance Plan for Your Business (Federal Trade Commission, June 2013) <<https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>> accessed 4 March 2017

Children's online privacy and freedom of expression (UNICEF May 2018) <[https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf)> accessed 17 November 2018.

Children's and young people's rights in the digital age (LSE July 2016) <<http://www.lse.ac.uk/media@lse/events/pdf/IAMCR16/CRDA-IAMCR16-Abstracts.pdf>> accessed 17 November 2018.

Chynoweth P, 'Legal Research in the Built Environment: A Methodological Framework' (University of Salford, Manchester) <http://usir.salford.ac.uk/12467/1/legal_research.pdf> accessed 3 December 2017

Clifford D, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster – Tracking the Crumbs of Online User Behaviour' (jipitec) <<https://www.jipitec.eu/issues/jipitec-5-3-2014/4095>> accessed 18 April 2017

Cohen P, 'Activision Buys Game Conversion Developer Beenox' (Macworld 25 May 2005) <<https://www.macworld.com/article/1044978/beenox.html>> accessed 23 January 2017

Cookies consent under the GDPR (EU GDPR Compliant) <<https://eugdprcompliant.com/cookies-consent-gdpr/>> accessed 18 May 2018

'Commission Wants to Simplify Life for SME's by Easing the Top 10 Most Burdensome EU Laws' (Europa, 2013) <http://Europa.eu/rapid/press-release_IP-13-188_en.htm> accessed 8 December 2015

Commissioner for Human Rights, 'Protecting Children's Rights in the Digital World: An Ever-Growing Challenge' (Europa, 29 April 2014) <<https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1?desktop=true>> accessed 7 February 2018

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union (European Commission, 2010) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609>> accessed 20 December 2015

Complexity of EU Law in the Domestic Implementing Process (Europa, 3 July 2014) <http://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf> accessed 31 March 2017

‘Complying with COPPA: Frequently Asked Questions’ (Federal Trade Commission) <<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>> accessed 8 May 2017

‘Complying with COPPA: Frequently Asked Questions’ (Federal Trade Commission, 20 March 2015) <<https://webcache.googleusercontent.com/search?q=cache:xn1ZBa1ByYoJ:https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2017

Conspicuous, Oxford Dictionary <<https://en.oxforddictionaries.com/thesaurus/conspicuous>> accessed 29 March 2018

‘Consumer Information’ (Federal Trade Commission) <<https://www.consumer.ftc.gov/articles/0042-online-tracking>> accessed 29 March 2017

Consumers: Online Tracking: Hearing on AB 370 (Muratsuchi) Before S. Comm. on the Judiciary, 2013–2014 Reg. Sess. (June, 18, 2013), <[leginfo. legislature.ca.gov](http://leginfo.ca.gov)> accessed 29 March 2017

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data <<https://rm.coe.int/1680078b37>> accessed 26 November 2015

'Cookies' (Europa) <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm> accessed 19 March 2017

Cookies and GDPR: what you need to know (Automated Intelligence 4 December 2017) < <https://www.automated-intelligence.com/news-and-events/blog/cookies-gdpr-need-know/>> accessed 21 May 2018

'Cookies and Similar Technologies' (ICO) <<https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>> accessed 19 March 2017

'Cookies: Leaving a Trail on the Web' (i.t.pie) <<http://www.itpie.co.uk/blog/cookies-leaving-a-trail-on-the-web>> accessed 26 April 2018

'Cortana and Privacy' (Microsoft) <<https://privacy.microsoft.com/en-US/windows-10-cortana-and-privacy>> accessed 9 October 2016

'Council of Europe Strategy for the Rights of the Child (2016–2021)' (Council of Europe, March 2016) <<https://rm.coe.int/168066cff8>> accessed 3 December 2017

Council of Europe, 'Protecting children's rights in the digital world: an ever-growing challenge' (Europa) < <https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1?desktop=true>> accessed 23 November 2018.

Court of Justice of the European Union 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid' (Europa, 2015) <http://curia.europa.eu/jcms/jcms/P_180250/> accessed 11 April 2016

Creative Europe, 'Video Game Development' (European Commission) <https://ec.europa.eu/programmes/creative-europe/media/video-game-development_en> accessed 6 February 2017

'Cross-Device Tracking' (Federal Trade Commission, January 2017) <https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf> accessed 30 March 2017

'Data Protection and Service Providers – New Obligations, Liabilities and Contract Changes Loom' (Out-Law.com, 2015) <<http://www.out-law.com/en/articles/2015/september/data-protection-and-service-providers---new-obligations-liabilities-and-contract-changes-loom/>> accessed 14 December 2015

Data Protection Bill [HL] 2017-19 <<https://services.parliament.uk/bills/2017-19/dataprotection.html>> accessed 22 January 2018

Data Protection Act 2018 (www.parliament.uk) <<https://services.parliament.uk/bills/2017-19/dataprotection.html>> accessed 17 June 2018

Data Protection Act 2018 (ico) <<https://ico.org.uk/for-organisations/data-protection-act-2018/>> accessed 17 June 2018

Data Retention (TechTarget February 2014) <<https://searchstorage.techtarget.com/definition/data-retention>> accessed 21 September 2017

'Department for Culture, Media and Sport Consultation: General Data Protection Regulation – Call for Views' (ICO) <<https://ico.org.uk/about-the-ico/consultations/department-for-culture-media-and-sport-consultation-general-data-protection-regulation-call-for-views/>> accessed 31 January 2018

Details of Treaty No. 108 (Council of Europe)
<<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>>
accessed 7 April 2016

Determining What Is Personal Data (ICO) <<https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>> accessed 8 April 2016

'Device ID' (Microsoft) <<https://docs.microsoft.com/en-us/windows-hardware/drivers/install/device-ids>> accessed 18 April 2018

'Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and through Their Mobile Devices' (Federal Trade Commission, 20 December 2016) <<https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively>>
accessed 2 February 2017

'Digital Heroin: Is the Internet Really a Drug? [Debate]' (ICDL Arabia, 14 February 2017) <<http://webcache.googleusercontent.com/search?q=cache:Z4a6-VBWgxIJ:onlinesense.org/digital-heroin/+&cd=4&hl=en&ct=clnk&gl=uk>> accessed 18 January 2018

'Digital Media and Children's Rights' (UN Committee on the Rights of Child, September 2014) <http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf> accessed 4 March 2018

'Discussion Paper Series: Children's Rights and Business in a Digital World' (UNICEF) <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 4 April 2018

'Dissenting Statement of Orson Swindle' (Federal Trade Commission) <<https://www.ftc.gov/public-statements/2000/07/dissenting-statement-commissioner-orson-swindle-ftcs-online-profiling>> accessed 28 June 2016

DLA Piper, 'EU Study on the Legal Analysis of a Single Market for the Information Society' (Europa, November 2009) <www.Europa.eu> accessed 28 December 2016

Donnelly C, 'Xbox Live Users Hit by Data Breach' (ITPro 2013) <<http://www.itpro.co.uk/data-leakage/19470/xbox-live-users-hit-data-breach>> accessed 29 March 2016

Dowty T and Korff D, 'Protecting the Virtual Child: The Law and Children's Consent to Sharing Personal Data' (ARCH, 2009) <http://www.northumbria.ac.uk/static/5007/hces/virtual_child.pdf> accessed 10 January 2016

Draper G, 'Writing and Readability Scores: It Matters' (Marketingprofs, 3 January 2014) <<http://www.marketingprofs.com/articles/2014/12377/writing-and-readability-scores-it-matters>> accessed 26 January 2018

Dubay W, 'Smart Language: Readers, Readability, and the Grading of Text' (Impact Information 2007) <<http://www.impact-information.com/impactinfo/newsletter/smartlanguage02.pdf>> accessed 26 January 2018

'Dynamic Internet Protocol Address' (Techopedia) <<https://www.techopedia.com/definition/28504/dynamic-internet-protocol-address-dynamic-ip-address>> accessed 18 April 2018

'The eBusiness Guide' (eBizMBA) <www.ebizmba.com/> accessed 11 March 2017

'EchoMetrix Inc.' (Federal Trade Commission, 30 November 2010) <<https://webcache.googleusercontent.com/search?q=cache:6QV5M1D8u4kJ:https://www.echo-metrix.com/>>

<http://www.ftc.gov/enforcement/cases-proceedings/102-3006/echometrix-inc+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2017

Eight in 10 auto businesses still in the dark over GDPR, says motor ombudsman (car dealer 23 May 2018) < <http://cardealermagazine.co.uk/publish/eight-10-auto-businesses-still-dark-gdpr-says-motor-ombudsman/151493>> accessed 17 June 2018

Electronic Arts Inc. Privacy Policy <<http://www2.ea.com/privacy-policy>> accessed 15 March 2017

Emerging Trends in Paint India Gaming Industry <[https://www.techsciresearch.com/admin/gall_content/2017/6/2017_6\\$thumbimg_114_Jun_2017_074442683.pdf](https://www.techsciresearch.com/admin/gall_content/2017/6/2017_6$thumbimg_114_Jun_2017_074442683.pdf)> accessed 23 January 2018

ESET (Enjoy Safer Technology) <<https://www.eset.com/int/>> accessed 10 February 2018

'EU Data Protection Reform: Where Are We – and What Can You Do to Prepare?' (Olswang) <http://www.olswang.com/media/48316310/olswang_s_top_12_eu_data_protection_reform.pdf> accessed 22 April 2017

'EU Kids Online' (LSE, 2016) <<http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>> accessed 7 February 2018

'EU Kids Online' (LSE) <<http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online>> accessed 29 April 2018

European Commission, '2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related

Frequently Asked Questions Issued by the US Department of Commerce (Notified under Document Number C(2000) 2441)' (Europa) <<http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520>> accessed 14 March 2017

EU referendum results (The Electoral Commission) <<https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information>> accessed 18 June 2018

European Commission, 'Data Protection: Commission Recognises Adequacy of Canadian Regime' (Europa, 14 January 2002) <http://Europa.eu/rapid/press-release_IP-02-46_en.htm?locale=en> accessed 15 November 2017

European Commission, 'EU-U.S. Privacy Shield' (Europa, July 2016) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf> accessed 14 March 2017

European Commission, 'Reform of EU Data Protection Rules' (Europa) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 21 December 2017

European Commission, 'Restoring Trust in Transatlantic Data Flows through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield' (Europa, 2016) <http://Europa.eu/rapid/press-release_IP-16-433_en.htm> accessed 12 April 2016

European Commission, 'The EU-U.S. Privacy Shield' (Europa) <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> accessed 14 March 2017

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (Council of Europe 4 November 1950) <<http://www.refworld.org/docid/3ae6b3b04.html>> accessed 24 March 2016

'European Data Protection Supervisor' (Europa) <https://edps.europa.eu/about-edps_en> accessed 19 August 2017

European Data Protection Supervisor 'Privacy Shield: More Robust and Sustainable Solution needed' (Europa, 30 May 2016) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf> accessed 14 March 2017

European Union (Withdrawal) Bill (HC Bill 5) <https://publications.parliament.uk/pa/bills/cbill/2017-2019/0005/cbill_2017-20190005_en_1.htm> accessed 22 January 2018

EU-U.S. Privacy Shield Framework Principles Issued by the US Department of Commerce' (Europa) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf> accessed 14 March 2017

'EU-U.S. Privacy Shield Solutions' (TRUSTe) <<https://www.trustarc.com/consumer-resources/privacy-shield/>> accessed 13 February 2017

Fact sheet: A summary of the rights under the Convention on the Rights of the Child (UNICEF) https://www.unicef.org/crc/files/Rights_overview.pdf accessed 16 November 2018

Fair L, 'What Vizio Was Doing behind the TV Screen' (Federal Trade Commission 6 February 2017) <<https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen>> accessed 30 March 2017

Farrukh A, Sadwick R and Villasenor J, 'Youth Internet Safety: Risks, Responses, and Research Recommendations' (Center for Technology Innovation at Brookings

October 2014) <https://www.brookings.edu/wp-content/uploads/2016/06/Youth-Internet-Safety_v07.pdf> accessed 6 February 2018

'Federal Trade Commission 2013 Privacy and Data Security Update' (Federal Trade Commission) <<https://www.ftc.gov/reports/privacy-data-security-update-2013>> accessed 1 March 2017

Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices <<https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf>> accessed 27 June 2016

Federal Trade Commission, 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business' <<https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>> accessed 29 March 2018

Federal Trade Commission, 'Protecting Kid's Privacy Online Reviewing the COPPA' (Federal Trade Commission 2 June 2010) <<https://www.ftc.gov/news-events/events-calendar/2010/06/protecting-kids-privacy-online-reviewing-coppa-rule>> accessed 12 May 2017

Federal Trade Commission, 'Protection Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers' (FTC March 2012) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>> accessed 31 January 2018

Federal Trade Commission, 'What We Do' (FTC) <<https://www.ftc.gov/about-ftc/what-we-do>> accessed 14 March 2018

Fisher T, 'Terabytes, Gigabytes, & Petabytes: How Big Are They?' (Lifewire, 20 September 2017) <<https://webcache.googleusercontent.com/search?q=cache:o8KdFrGKADEJ:https://>

www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169+&cd=3&hl=en&ct=clnk&gl=uk> accessed 27 October 2017

'Flesch Reading Ease Readability Formula' (Readability Formulas) <<http://www.readabilityformulas.com/flesch-reading-ease-readability-formula.php>> accessed 6 March 2017

Frank J, 'Microsoft's Commitments, Including DPA Cooperation, under the EU-U.S. Privacy Shield' (Microsoft, 2016) <<https://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/>> accessed 12 April 2016

'Free Online Games: Top Gaming Resource' (TechGlamour) <<http://techglamour.com/online-free-games-gaming-resources/#sthash.LD8L65I0.dpuf>> accessed 23 January 2017

Fry E, "'Readability' Reading Hall of Fame Book' (International Reading Assn 2006) <<http://www.impact-information.com/impactinfo/fryreadability.pdf>> accessed 26 January 2018

'FTC Grants Approval for New COPPA Verifiable Parental Consent Method' (Federal Trade Commission, 19 November 2015) <<https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>> accessed 1 March 2017

Furtsch J, 'COPPA Is Not Just for kid's Websites Anymore' (iapp, 28 October 2014) <<https://iapp.org/news/a/coppa-is-not-just-for-kids-websites-anymore/>> accessed 5 March 2017

Gaudiosi J, 'The 10 Most Successful States for Video Game Development' *Fortune* (24 February 2015) <<http://fortune.com/2015/02/24/10-successful-states-video-game-development/>> accessed 22 January 2017

GDPR consent guidance (ICO) < <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/>> accessed 19 May 2018

'GDPR Overview: Site Portal' <<https://www.eugdpr.org/>> accessed 16 March 2018

GDPR – where guidance is needed (Data protection network) <https://www.dpnetwork.org.uk/opinion/gdpr-guidance-needed/> accessed 17 June 2018

General Assembly, 'Resolution 68/167 The Right to Privacy in the Digital Age' (United Nations, 2014) <<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>> accessed 25 March 2016

Gera E, 'Star Wars: The Old Republic Continues to Stay Afloat with Over 1M Monthly Players' (Polygon Vox Media, 14 August 2014) <<http://www.polygon.com/2014/8/14/6001503/star-wars-the-old-republic-2014-players-ea-bioware>> accessed 23 January 2017

Gilbert F, 'EU Data Protection Overhaul: New Draft Regulation' (Global Privacy Book) <<http://www.globalprivacybook.com/blog-european-union/223-eu-data-protection-overhaul-new-draft-regulation>> accessed 10 December 2015

Global Kids Online <<http://globalkidsonline.net/>> accessed 25 April 2018

Global Kids Online Research Toolkit – Quantitative Guide <<http://globalkidsonline.net/>> accessed 25 April 2018

Goel V, 'Facebook Tinkers with User's Emotions in News Feed Experiment, Stirring Outcry' (*The New York Times*) 29 June 2014) <<https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html>> accessed 2 February 2018

Gorge M, 'The Implications for Storage of EU Data Protection Regulation' (ComputerWeekly.com) <<http://www.computerweekly.com/feature/The-implications-for-storage-of-EU-data-protection-regulation>> accessed 28 December 2016

'Governing Law and Jurisdiction Clauses' (Lexology) <<http://www.lexology.com/library/detail.aspx?g=469b7d6f-4f8c-44cb-9f10-dcdd1edf20bf>> accessed 6 March 2017

Government of Canada Moves to Enhance Privacy of Individuals During Commercial Transactions (Industry Canada, 29 September 2011) <<https://www.canada.ca/en/news/archive/2011/09/government-canada-moves-enhance-privacy-individuals-during-commercial-transactions.html>> accessed 2 March 2017

Greer S, 'The Margin of Appreciation: Interpretation and Discretion under the European Convention on Human Rights' (Council of Europe 2000) <[http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17\(2000\).pdf](http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf)> accessed 30 March 2016

Guidance: What to Expect and When (ICO) <<https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/guidance-what-to-expect-and-when/>> accessed 3 December 2017

Gustafsson J, 'Single Case Studies vs. Multiple Case Studies: A Comparative Study (2017) <<http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf>> accessed 1 May 2018

'Hackers Leak Details of 13k Users of PlayStation, Xbox and Amazon' *The Telegraph* (2014) <www.telegraph.co.uk> accessed 29 March 2016

'Hackers Steal Millions of Minecraft Passwords' (BBC News, 29 April 2016) <<http://www.bbc.co.uk/news/technology-36168860>> accessed 27 October 2017

Hagenmeier J, 'Invest in Video Gaming: A Booming Industry in Emerging Markets' (Day Trading Academy, 6 May 2014) <<https://webcache.googleusercontent.com/search?q=cache:E2XjWAA5fysJ:https://daytradingacademy.com/invest-video-games-booming-industry-emerging-markets/+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 23 January 2018

Hague C and Payton S, 'Digital Literacy across the Curriculum' (Futurelab, 2010) <<https://www.nfer.ac.uk/publications/FUTL06/FUTL06.pdf>> accessed 2 February 2018

Harris K, 'Making Your Privacy Practices Public' (California Department of Justice, May 2014) <https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf> accessed 30 March 2017

Harry Potter <<https://www.warnerbros.co.uk/games/harry-potter-spells>> accessed 31 May 2017

Hasty R, Nagel T and Subjally M White and Case, 'Data Protection Law in the USA' (A4ID, August 2013) <https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf> accessed 20 June 2016

'Have Ontario and Quebec Eclipsed Vancouver in the Video Game Industry?' <<http://studymagazine.com/2013/07/29/have-ontario-and-quebec-eclipsed-vancouver-in-the-video-game-industry/>> accessed 18 August 2017

Have Your say: Should We Restrict children's Social Media Use? (Sky News, 10 March 2018) <<https://news.sky.com/story/have-your-say-should-we-restrict-childrens-social-media-use-11283498>> accessed 10 March 2018

Hilton <<http://www3.hilton.com/en/index.html>> accessed 20 April 2018

Hilton Honors <<http://hiltonhonors3.hilton.com/en/policy/global-privacy-statement/index.html>> accessed 20 April 2018

Hogan Lovells, 'California Continues to Shape Privacy and Data Security Standards' (iapp) <<https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/>> accessed 1 October 2013

Hordern V, 'Consent – the Silver Bullet' (2013) <<http://www.fieldfisher.com/publications/2013/02/consent-the-silver-bullet>> accessed 16 January 2016

House of Lords European Union Committee, 'Brexit: the EU Data Protection Package' (parliament.uk, 18 July 2017) <<https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf>> accessed 22 January 2018

Hsiao M and others, 'Parents and the Internet: Privacy Awareness, Practices and Control' (Amcis, 2007) <<https://pdfs.semanticscholar.org/7a0b/58dfa89fd3b05a221f76006842b3515283c2.pdf>> accessed 17 November 2017

'HTTP Cookies' <<https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>> accessed 13 April 2018

Hunt A and Wheeler B, 'Brexit: All You Need to Know about the UK Leaving the EU' (BBC News, 25 April 2017) <<http://www.bbc.co.uk/news/uk-politics-32810887>> accessed 16 May 2017

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (EDPS, 2014) <<https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents>>

[/EDPS/Publications/Speeches/2014/14-09-15 Article EUI EN.pdf](#)> accessed 7 April 2016

ICO <<https://ico.org.uk/for-the-public/>> accessed 29 April 2018

‘ICO GDPR Guidance’ (ICO, 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed 14 April 2017

‘Impact Assessment’ (Ministry of Justice, 2012) <<https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf>> accessed 9 December 2015

‘Interland: Be Internet Awesome’ (fwa, June 2017) <<https://thefwa.com/cases/interland-be-internet-awesome>> accessed 9 March 2018

‘Invalid’ (Europa, 6 October 2015) <http://curia.Europa.eu/jcms/jcms/P_180250/> accessed 14 March 2017

‘Is Canada Safe from the Safe Harbour Decision?’ (Lexology, 13 December 2015) <<https://www.lexology.com/library/detail.aspx?g=cf0e7076-8930-4b74-9493-ca5522c8e5b2>> accessed 15 November 2017

Katsarova I, ‘Protection of Minors in the Media Environment EU Regulatory Mechanisms’ (Europa, 18 March 2013) <[http://www.europarl.Europa.eu/RegData/bibliotheque/briefing/2013/130462/LDM_BRI\(2013\)130462_REV1_EN.pdf](http://www.europarl.Europa.eu/RegData/bibliotheque/briefing/2013/130462/LDM_BRI(2013)130462_REV1_EN.pdf)> accessed 31 January 2018

‘Kid’s Privacy/COPPA Assessments & Certifications’ (TRUSTe) <<https://www.trustarc.com/products/coppa-certification/>> accessed 7 March 2017

Kilkelly U, 'A Guide to the Implementation of Article 8 of the European Convention on Human Rights' (Council of Europe) <[http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01\(2003\).pdf](http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01(2003).pdf)> accessed 30 March 2016

King Privacy Policy <<http://about.king.com/consumer-terms/terms/en>> accessed 15 March 2017

Kirk J, 'Adobe Flash Cookies Pose Vexing Privacy Questions' (Pcworld, 11 August 2009) <<http://www.pcworld.com/article/169985/article.html>> accessed 18 March 2017

Klosek J, 'Data Protection in the Information Age' (Quorum Books, 2000)

'Self-Regulation and privacy online' (Federal Trade Commission, July 1999) <<https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-online-federal-trade-commission-report-congress/1999self-regulationreport.pdf>> accessed 14 March 2017

Lancefield D, 'The Department for Culture, Media and Sport Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the UK Electronic Communications Framework' (Department for Culture, Media and Sport) <http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf> accessed 23 January 2016

'Language Barrier' *The Law Society Gazette* (10 June 2004) <<https://www.lawgazette.co.uk/news/language-barrier/42217.article>> accessed 26 January 2018

Lee P, 'How Do EU and US Privacy Regimes Compare?' (fieldfisher, 5 March 2014) <<http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare/>> accessed 10 November 2017

Lee P, 'The ambiguity of unambiguous consent under the GDPR' (fieldfisher 7 June 2016) <<https://privacylawblog.fieldfisher.com/2016/the-ambiguity-of-unambiguous-consent-under-the-gdpr>> accessed 20 May 2018

Legitimate Interests (ICO) <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>> accessed 5 April 2018

Lenhart A and others, 'Teens, Videogames and Civics' (Pew Research Centre, 16 September 2008) <<http://www.pewinternet.org/2008/09/16/teens-video-games-and-civics/>> accessed 27 October 2017

Levin K, 'A Look at the Protection of Children's Personal Information in an Online Context' (Lexology, 3 November 2011) <<https://www.lexology.com/library/detail.aspx?g=9decc24d-ac5f-4bbf-b8cc-6b9710523480>> accessed 10 November 2017

Livingston B, 'How Trustworthy Is the TRUSTe Privacy Logo' (datamation, 10 October 2006) <http://www.datamation.com/columns/executive_tech/article.php/3637066/How-Trustworthy-Is-the-TRUSTe-Logo.htm> accessed 28 March 2017

Livingstone S and others, 'Digital Literacy and Safety Skills' (EU Kids Online) <[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIReports/DigitalSkillsShortReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/DigitalSkillsShortReport.pdf)> accessed 2 February 2018

Livingstone S and others, 'Risks and Safety for Children on the Internet: The UK Report' (The London School of Economics and Political Science, December 2010) <[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/National%20reports/UKReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf)> accessed 17 November 2017

Livingstone S and others, 'Risks and Safety for Children on the Internet: The UK Report' (The London School of Economics and Political Science, December 2010) <[http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/National%20reports/UKReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf)> accessed 17 November 2017

Livingstone S and Third A, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (SAGE Journals, 10 May 2017) <<http://journals.sagepub.com/doi/full/10.1177/1461444816686318>> accessed 9 February 2018

Livingstone S, Haddon L, 'Introduction-Kids Online: Opportunities and Risks for Children' (Policy Press 2009) <[http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_\(LSERO\).pdf](http://eprints.lse.ac.uk/30130/1/Kids_online_introduction_(LSERO).pdf)> accessed 23 January 2016

Livingstone S, Mascheroni G and Staksrud E, 'Developing a Framework for Researching Children's Online Risks and Opportunities in Europe' (EU Kids Online, November 2015) <http://eprints.lse.ac.uk/64470/1/_lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU%20Kids%20Online_Developing%20framework%20for%20researching_2015.pdf> accessed 3 December 2017

Longfield A, 'Growing Digital One Year On' (The Children's Commissioner's Office, 6 February 2018) <<https://www.childrenscommissioner.gov.uk/2018/02/06/growing-up-digital-one-year-on/>> accessed 24 February 2018

Lord N, 'Browser Security Settings for Chrome, Firefox and Internet Explorer: Cybersecurity 101' (Veracode, 22 March 2013) <<https://www.veracode.com/blog/2013/03/browser-security-settings-for-chrome-firefox-and-internet-explorer>> accessed 24 October 2016

Lords Say Digital Skills Will Make or Break the UK (Parliament, 17 February 2015) <<https://www.parliament.uk/business/committees/committees-a-z/lords-select/digital-skills-committee/news/report-published/>> accessed 9 March 2018

Lott J, Schall D and Peters K, 'Actionscript 3.0 Cookbook' (O'Reilly, 2006) <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.7830&rep=rep1&type=pdf>> accessed 18 March 2017

McCarthy C, 'Electronic Arts pays \$860 million for BioWare, Pandemic Studios' (cnet, 1 October 2007) <<https://www.cnet.com/news/electronic-arts-pays-860-million-for-bioware-pandemic-studios/>> accessed 23 January 2017

McDonald A and Cranor L, 'The Cost of Reading Privacy Policies' (2009) 4(3) I/S: A Journal of Law and Policy for the Information Society <<http://www.is-journal.org/>> accessed 20 January 2016

McGoogan C, 'Hackers Steal 2.5 Million PlayStation and Xbox Players' Details in Major Breach' *The Telegraph* (1 February 2017) <<https://www.telegraph.co.uk/technology/2017/02/01/hackers-steal-25-million-playstation-xbox-players-details-major/>> accessed 4 April 2018

McGowan J and Shahab L 'Psychological Aspects of Tobacco Control' (Oxford University Press July 2017) <<http://psychology.oxfordre.com/view/10.1093/acrefore/9780190236557.001.0001/acrefore-9780190236557-e-126>> accessed 2 May 2017

Madden M and others, 'Teens, Social Media and Privacy' (Pew Research Center, 21 May 2017) <<http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>> accessed 3 December 2017

Madhavan M, 'How League of Legends Became the Most Popular Game in the World' (Referral Candy blog, 6 January 2016) <<https://www.referralcandy.com/blog/league-of-legends-word-of-mouth-marketing/>> accessed 3 December 2017

Mahler T, Fitsch L and Josang A, 'Privacy Policy Referencing' (2010) <<http://folk.uio.no/josang/papers/JFM2010-TrustBus.pdf>> accessed 17 December 2015

'Making Your Privacy Practices Public' (California Department of Justice, May 2014) <https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf> accessed 6 March 2017

Marmor A, 'What Is the Right to Privacy' (2015) 43(1) *Philosophy and Public Affairs* <<http://onlinelibrary.wiley.com/doi/10.1111/papa.12040/full>> accessed 21 November 2015

Marsan C, '15 Worst Internet Privacy Scandals of All Time' (NETWORKWORLD, 26 January 2012) <<http://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html>> accessed 18 November 2015

Meikle A, 'The Gaming Industry Continues to Thrive: Outselling Movies by a Good Margin' (*mygaming*, 15 October 2015) <<https://mygaming.co.za/news/business/82528-the-gaming-industry-continues-to-thrive-outselling-movies-by-a-good-margin.html>> accessed 7 February 2018

Meyer R, 'Everything We Know about Facebook's Secret Mood Manipulation Experiment' *The Atlantic* (24 June 2014) <<https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>> accessed 2 February 2018

Microsoft Privacy Policy <<https://privacy.microsoft.com/en-us/privacystatement>> accessed 15 March 2017

Miller C, 'Google to Pay \$17 Million to Settle Privacy Case' *The New York Times* <<http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?mcubz=1>> accessed 21 August 2017

Miniclip Privacy Policy <<http://www.miniclip.com/android/privacy-policy/>> accessed 15 March 2017

'More than 140,000 Children Could Be Victims of Identity Fraud Each Year' (id:analytics, 12 July 2011) <<http://www.idanalytics.com/press-release/140000-children-victims-identity-fraud-year/>> accessed 28 October 2017

'Most Played PC Games on Gaming Platform Raptr in November 2015, by Share of Playing Time' (statista 2015) <<https://www.statista.com/statistics/251222/most-played-pc-games/>> accessed 22 January 2017

Nahmias J <<http://www.nahmiaslaw.com/about/>> accessed 21 March 2018

Nahmias J, 'The EULA: What It Does, How It Works (and, What Does EULA Even Mean?)' (Nahmiaslaw, 23 November 2011) <<http://www.nahmiaslaw.com/the-eula-what-it-does-how-it-works-and-what-does-eula-even-mean/>> accessed 16 May 2016

'New Report Predicts Future Technology Trends among Children and Young People' (Childwise, 2015) <<http://www.childwise.co.uk/reports.html>> accessed 27 November 2015

Nichols W, 'Advertising Analytics 2.0' *Harvard Business Review* (March 2013) <<https://hbr.org/2013/03/advertising-analytics-20>> accessed 18 March 2017

Nolte N and Werkmeister C, 'Data Protection in Germany: An Overview' (Practical Law) <<http://uk.practicallaw.com/3-502-4080>> accessed 15 May 2016

'Canada's Video Game Industry in 2015' (Nordicity, August 2015) <<http://www.nordicity.com/media/20151210faaebhea.pdf>> accessed 23 January 2017

NSPCC <<https://www.nspcc.org.uk/>> accessed 2 February 2018

NSPCC and O2 <<https://www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership/>> accessed 2 February 2018

Nutt C, Canada's Game Dev Industry Grows: 472 Studios, 20,400 People (Gamasutra, 16 November 2015) <http://www.gamasutra.com/view/news/259511/Canadas_game_dev_industry_grows_472_studios_20400_people.php> accessed 23 January 2017

O2 <<https://webcache.googleusercontent.com/search?q=cache:SMtn5342EusJ:https://www.o2.co.uk/+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 2 February 2018

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>> accessed 20 November 2015

'Ofcom Report on Internet Safety Measures' (Ofcom, 12 January 2015) <https://www.ofcom.org.uk/data/assets/pdf_file/0016/31732/Third-internet-safety-report-January-2015.pdf> accessed 6 February 2018

Office of the Data Protection Commissioner, 'Article 29 Working Party' (Data Protection Commissioner) <<https://www.dataprotection.ie/docs/Article-29-Working-Party/u/181.htm>> accessed 5 April 2018

'Online Abuse Facts and Statistics' (NSPCC) <<https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/facts-statistics/>> accessed 6 February 2018

Online Privacy Law: Canada (Library of Congress, 6 May 2015)
<<https://www.loc.gov/law/help/online-privacy-law/2017/canada.php>> accessed 1
March 2017

'Opinion 15/2011 of the Article 29 Working Party on the Definition of Consent'
(Europa, 2011)
<http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=3&hl=en&ct=clnk&gl=uk> accessed 8 January
2016

'Opinion 2/2009 on the Protection of Children's Personal Data (Children's Guidelines
and the Special Case of Schools)' (Europa, 2009)
<http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=2&hl=en&ct=clnk&gl=uk> accessed 10
January 2016

'Opinion 2/2010 Online Behavioural Advertising' (Europa, 2010)
<https://webcache.googleusercontent.com/search?q=cache:J1qvDBpz-SgJ:https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/nota_as_prensa/common/junio/WP171en.pdf+&cd=1&hl=en&ct=clnk&gl=uk> accessed
22 January 2016

'Opinions and Recommendations' (Europa)
<http://webcache.googleusercontent.com/search?q=cache:T2kmKrBIUbgJ:ec.Europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm+&cd=1&hl=en&ct=clnk&gl=uk> accessed 20 March
2017

Osborne C, 'Millions of Game Accounts Exposed in Data Breach, Responsibility Thrown to the Wind' (ZDNet, 20 April 2017) <<https://www.zdnet.com/article/amid-data-breach-responsibility-thrown-to-the-wind/>> accessed 17 November 2017

'Overview of China's Cybersecurity Law' (KPMG) <<https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>> accessed 23 January 2018

Oxford Dictionary <<https://en.oxforddictionaries.com/definition/dataveillance>> accessed 13 April 2018

Pareigat T, 'Maintaining Customer Confidence Online' (ABA Bank Compliance, March/April 2001) <<https://congressional.proquest.com/central>> accessed 10 January 2017

'Persistent identifiers' (USGS) <<https://www2.usgs.gov/datamanagement/preserve/persistentIDs.php>> accessed 1 March 2017

Piltz C, 'The European Data Protection Law and Minors – No Legal Certainty' (German IT Law, 2014) <<http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty/>> accessed 12 January 2017

'PIPEDA Review Discussion Document' (Privacy Commissioner of Canada, July 2006) <https://www.priv.gc.ca/media/1312/pipeda_review_060718_e.pdf> accessed 14 May 2017

Princess Isabella: A Witch's Curse <<https://www.giantbomb.com/princess-isabella-a-witches-curse/3030-46348/>> accessed 15 November 2017

'Privacy and Data Security Update' (Federal Trade Commission, 2014)
<https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf> accessed 27 June 2016

'Privacy and Data Security Update' (Federal Trade Commission, January 2016)
<<https://www.ftc.gov/reports/privacy-data-security-update-2015>> accessed 1 March 2017

'Privacy Concerns on Cookies' <<http://www.allaboutcookies.org/privacy-concerns/>>
accessed 20 January 2016

'Privacy Modelling Tool' (watech) <https://watech-beta.herokuapp.com/user_guide> accessed 5 March 2017

'Privacy Online' (Federal Trade Commission)
<<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>> accessed 6 March 2017

'Privacy Online: A Report to Congress' (Federal Trade Commission, June 1998)
<<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>> accessed 11 July 2016

'Privacy Online: Fair Information Practices in the Electronic Marketplace' (Federal Trade Commission, May 2000)
<<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>> accessed 2 February 2017

'Privacy Shield Principles'
<<https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>> accessed 6 April 2018

'Privacy Shield Principles Notice 1(a)(i)' <<https://www.privacyshield.gov/article?id=1-NOTICE>> accessed 14 March 2017

Proposal for an ePrivacy Regulation (europa) < <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>> accessed 24 June 2018

Protalinski E, '8.24 Million Gamigo Passwords Leaked after Hack' (ZD Net, 23 July 2012) <<http://www.zdnet.com/article/8-24-million-gamigo-passwords-leaked-after-hack/>> accessed 17 November 2017

'Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers, Preliminary Staff Report' (Federal Trade Commission, 2010) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>> accessed 7 March 2017

'Q&A: Charter of Fundamental Rights' (BBC, 2007) <<http://news.bbc.co.uk/1/hi/world/europe/6225580.stm>> accessed 31 March 2016

Raman M, 'Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime' (Department of Justice) <<http://www.justice.gov/iso/opa/ola/witness/02-04-14-cmr-raman-testimony-re-privacy-in-the-digital-age-preventing-data-breac.201427115.pdf>> accessed 25 March 2016

Ramirez E, 'ANNEX IV' (Europa, 23 February 2016) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-4_en.pdf> accessed 28 March 2017

Ramirez E, 'Federal Trade Commission' (Federal Trade Commission, 9 January 2017) <https://www.ftc.gov/system/files/documents/public_statements/1049563/ramirez_swiss_privacy_shield_letter.pdf> accessed 1 March 2017

Reform of EU Data Protection Rules' (Europa) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 7 April 2016

'Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Records, Computers and the Rights of Citizens)' <<https://www.hsd1.org/?view&did=479784>> accessed 5 March 2017

'Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing' (Office of the Privacy Commissioner of Canada, May 2011) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/report_201105/> accessed 2 March 2017

'Requirements of Participation' (Privacy Shield Framework) <<https://www.privacyshield.gov/article?id=Requirements-of-Participation>> accessed 28 March 2017

'Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework' (Department for Culture, Media and Sport, April 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77641/PwC_Internet_Cookies_final.pdf> accessed 19 March 2017

'Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings' (Federal Trade Commission, 12 November 2013) <<https://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf>> accessed 28 June 2016

'Results' (BBC News) <http://www.bbc.co.uk/news/politics/eu_referendum/results> accessed 16 May 2017

Retail Tracking Firm Settles FTC Charges It Misled Consumers about Opt Out Choices (Federal Trade Commission, 23 April 2015) <<https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers>> accessed 30 March 2017

'Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted' (Channel 4 News, 28 March 2018) <<https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted>> accessed 29 March 2018

'Revised Children's Online Privacy Protection Rule Goes into Effect Today' (Federal Trade Commission, 1 July 2013) <<https://webcache.googleusercontent.com/search?q=cache:iwahN-q3VZoJ:https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 30 March 2017

Riot Games Privacy Policy <<http://euw.leagueoflegends.com/en/legal/privacy#expand>> accessed 15 March 2017

Rogers K, 'Video Games Could Increase Children's Risk of Identity Theft' (Fox News, 31 August 2011) <<http://www.foxbusiness.com/features/2011/08/31/video-games-could-increase-childrens-risk-identity-theft.html>> accessed 28 October 2017

Rudgard S, 'Origins and Historical Context of Data Protection Law' <https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf> accessed 24 February 2018

Sandberg E, 'More Parents Giving Their Kids Credit Cards' (creditcards.com, 23 June 2017) <<https://webcache.googleusercontent.com/search?q=cache:BsM0I-WhREEJ:https://www.creditcards.com/credit-card-news/more-parents-giving-kids-credit-cards.php+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 24 February 2018

Saskatchewan R, 'Resolution of Canada's Privacy Commissioners and Privacy Oversight Officials' (Office of the Privacy Commissioner of Canada, 4 June 2008) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_080604/?wbdisable=true> accessed 22 February 2018

Sathiyamurthi S, 'The Struggle for Privacy and the Survival of the Secured in the IT Ecosystem' (ISACA 2011) <<http://www.isaca.org/Journal/archives/2011/Volume-2/Pages/The-Struggle-for-Privacy-and-the-Survival-of-the-Secured-in-the-IT-Ecosystem.aspx>> accessed 25 March 2016

Schwartz P, 'Comparative Contractual Privacy Law: The U.S. and EU' <https://www.law.uchicago.edu/files/file/schwartz_comparative_contractual_privacy_law.pdf> accessed 15 November 2017

'Sears Settles FTC Charges Regarding Tracking Software' (Federal Trade Commission, 4 June 2009) <<https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software>> accessed 2 February 2017

Self-Regulation and Privacy Online (Federal Trade Commission, July 1999) <<https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-online-federal-trade-commission-report-congress/1999self-regulationreport.pdf>> accessed 14 March 2017

Shelton D, 'California Adopts Do-Not-Track Disclosure Law: A.B. 370 Amends the California Online Privacy Protection Act (CalOPPA) to Require New Privacy Policy Disclosures for Websites, Online Services and Mobile Apps about Behavioral Tracking' <<http://www.alstonprivacy.com/california-adopts-do-not-track-disclosure-law-a-b-370-amends-the-california-online-privacy-protection-act-caloppa-to-require-new->

[privacy-policy-disclosures-for-websites-online-services-and-mobile/](#)> accessed 7 March 2017

Simon S, 'Data Mining Your Children' (Politico, 2014) available at: http://www.politico.com/story/2014/05/data-mining-your-children-106676_Page2.html> accessed 24 December 2016

'SLDS Spotlight Privacy Classifications for Washington's Data' (SLDS) <https://nces.ed.gov/programs/slds/pdf/Privacy_Classifications_for_Washingtons_Data_May2015.pdf> accessed 5 March 2017

Soltani A, 'Flash Cookies and Privacy' (AshkanSoltani, 2009) <<http://ashkansoltani.org/2009/08/09/flash-cookies-and-privacy/>> accessed 20 January 2016

Sonia Livingstone, 'A Method for Researching Global Kids Online – Understanding Children's Well-Being and Rights in the Digital Age' (Global Kids Online November 2016) <<http://globalkidsonline.net/>> accessed 25 April 2018

Sporck L, 'The 8 Worst Data Breaches of All Time' (Network Security, 2016) <<http://www.networkcomputing.com/net-security/8-worst-data-breaches-all-time/23644893>> accessed 25 March 2016

State of California Department of Justice, 'About the Office of the Attorney General' <<https://oag.ca.gov/office>> accessed 24 January 2017

'Static v. Dynamic IP Address' (Google Fiber) <<https://support.google.com/fiber/answer/3547208?hl=en>> accessed 1 April 2017

Stewart, J., 'Recalibrating the Flesch Readability Index for the Twenty-first Century' <http://www.academia.edu/30700337/Recalibrating_the_Flesch_Readability_Index_for_the_Twenty-first_Century> accessed 16 November 2018

Stratford SJ and Stratford J, 'Data Protection and Privacy in the United States and Europe' (Iassist, 1998) <<http://www.iassistdata.org/sites/default/files/igvol223stratford.pdf>> accessed 20 June 2016

'Stronger Data Protection Rules for Europe: the EU Adopts the Data Protection Reform Package' (Europa, 2015) <[http://europa.eu/rapid/press-release MEMO-15-6385_en.htm](http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm)> accessed 28 December 2015

Sullivan F, 'Is Online Gaming Safe?' (Cloudwards, 12 June 2017) <<https://www.cloudwards.net/is-online-gaming-safe/>> accessed 17 November 2017

Sumroy R, 'Data Protection and Direct Marketing: Child's Play' (Slaughter and May, March 2006) <<https://www.slaughterandmay.com/media/39158/marketing%20part%203.pdf>> accessed 15 May 2016

Supercell Privacy Policy <<http://supercell.com/en/privacy-policy/>> accessed 15 March 2017

Sweeney M, 'What Is PII, Non-PII, and Personal data?' (7Suite, 7 September 2017) <<https://7suite.com/2016/09/what-is-pii-personal-data/>> accessed 1 April 2017

'T.J. Maxx Theft Believed Largest Hack Ever' (Nbcnews.com, 2007) <http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever/> accessed 29 March 2016

'Taking Action – Data Protection' (ICO) <<https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>> accessed 24 January 2018

Taylor A, 'International Transfers of Personal Data' (Seqlegal, 20 January 2008) <<https://seqlegal.com/blog/international-transfers-personal-data>> accessed 15 March 2017

'Technology and Society' (TILTS) <<https://www.tilburguniversity.edu/webwijs/show/e.kosta-2/>> accessed 24 January 2018

'The "Durant" Case and Its Impact on the Interpretation of the Data Protection Act 1998' (Information Commissioner) <<http://www.nhsgrampian.org/grampianfoi/files/DurantCase.pdf>> accessed 6 December 2015

'The App Analytics and App Data Industry Standard' (App Annie) <<https://www.appannie.com/>> accessed 21 February 2017

'The Biggest Entertainment Markets in the World' (Business Tech, 31 May 2015) <<https://webcache.googleusercontent.com/search?q=cache:iq33Zf5jsQUJ:https://businessstech.co.za/news/lifestyle/88472/the-biggest-entertainment-markets-in-the-world/+&cd=1&hl=en&ct=clnk&gl=uk>> accessed 27 October 2017

The Data Protection Bill 2017 <<https://www.gov.uk/government/collections/data-protection-bill-2017>> accessed 14 January 2018

'The EU-U.S. Privacy Shield' (Itic, 2016) <<http://www.itic.org/safeharbor>> accessed 11 April 2016

The Federal Council, 'Swiss-US Privacy Shield: Better Protection for Data Transferred to the USA' (The Federal Council) <<https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html>> accessed 14 March 2017

‘The History of the General Data Protection Regulation’ (Europa) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 11 December 2017

‘The Protection of Children Online’ (OECD, 2012) <https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf> accessed 21 February 2018

‘The Right to Data Portability’ (ICO) <<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/>> accessed 21 September 2017

‘The UK’s Independent Authority Set Up to Uphold Information Rights in the Public Interest, Promoting Openness by Public Bodies and Data Privacy for Individual’ (ICO) <<https://ico.org.uk/>> accessed 30 June 2017

The White House, ‘Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights’ <<https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b>> accessed 31 January 2018

Third A and others. ‘Children’s Rights in the Digital Age’ (UNICEF) <[https://www.unicef.org/publications/files/Childrens Rights in the Digital Age A Download from Children Around the World FINAL.pdf](https://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf)> accessed 9 February 2018

‘Top 100 Countries by Game Revenues’ (newzoo) <<https://newzoo.com/insights/rankings/top-100-countries-by-game-revenues/>> accessed 11 March 2017

‘TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program’ (Federal Trade Commission, 17 November 2014) <<https://webcache.googleusercontent.com/search?q=cache:ukbYgSaiy4sJ:https://w>

www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its+&cd=1&hl=en&ct=clnk&gl=uk> accessed 28 March 2017

'TRUSTed Websites Privacy Certification' (TRUSTe)
<<https://www.trustarc.com/privacy-certification-standards/>> accessed 14 March 2017

'Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act' (Federal Trade Commission, 17 December 2015)
<<https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens>> accessed 1 March 2017

'U.S. Gaming Trends Report' (Adobe 12 October 2015)
<<https://www.slideshare.net/adobe/us-gaming-trends-report/1>> accessed 7 February 2018

'Ubisoft Montreal' <<http://montreal.ubisoft.com/en/>> accessed 23 January 2017

'UK Data Protection Regulator Is "Ineffective," Says Research' (UEA)
<http://www.uea.ac.uk/about/media-room/press-release-archive/-/asset_publisher/a2jEGMiFHPhv/content/uk-s-data-protection-regulator-is-ineffective-says-research> accessed 24 January 2018

'UK Information Commissioner's Advice on the Use of Cookies and Similar Technologies for Storing Information under the New Rules' (ICO, May 2012)
<https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf> accessed 20 January 2016

UN Committee on the Rights of the Child, 'Report of the 2014 Day of General Discussion "Digital Media and Children's Rights"' (OHCHR)

<http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf> accessed 3 December 2017

UN General Assembly Resolution 45/95 of 14 December 1990 Guidelines for the Regulation of Computerized Personal Data Files 1990 <<http://www.un.org/documents/ga/res/45/a45r095.htm>> accessed 28 November 2015

UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3 <<http://www.refworld.org/docid/3ae6b38f0.html>> accessed 4 November 2017
accessed 9 February 2018

UN General Assembly, International Covenant on Civil and Political Rights (United Nations, 16 December 1966) <<http://www.refworld.org/docid/3ae6b3aa0.html>> accessed 9 May 2017

United Kingdom (Europa) < https://europa.eu/european-union/about-eu/countries/member-countries/unitedkingdom_en> accessed 22 June 2018

‘United Nations Treaty Collection’ <https://webcache.googleusercontent.com/search?q=cache:nr6kif9nff4J:https://treaties.un.org/Pages/ViewDetails.aspx%3Fsrc%3DIND%26mtdsg_no%3DIV-11%26chapter%3D4%26lang%3Den+&cd=1&hl=en&ct=clnk&gl=uk> accessed 14 April 2018

United State Senate, ‘Hearing: An Examination of Children’s Privacy: New Technologies and the Children’s Online Privacy Protection Act’ (29 April 2010) <<https://www.gpo.gov/fdsys/pkg/CHRG-111shrg66284/pdf/CHRG-111shrg66284.pdf>> accessed 31 January 2018

'US Department of Commerce' (Europa, 2004)
<http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf> accessed 15 April 2016

'Use of Cookies and Similar Technology' (Adobe, 16 June 2016)
<<http://www.adobe.com/uk/privacy/cookies.html>> accessed 18 March 2017

'Valve Privacy Policy' <http://store.steampowered.com/privacy_agreement/>
accessed 15 March 2017

'Video Game Companies Are Collecting Massive Amounts of Data about You' (thestar.com) <<https://www.thestar.com/news/canada/2015/12/29/how-much-data-are-video-games-collecting-about-you.html>> accessed 15 March 2017

Waugh R, 'League of Legends Players Warned after Major Security Breach' (welivesecurity, 22 August 2013)
<<https://www.welivesecurity.com/2013/08/22/league-of-legends-players-warned-after-major-security-breach/>> accessed 28 October 2017

'What Is COPPA' (TechTarget, May 2010)
<<http://searchcrm.techtarget.com/definition/COPPA>> accessed 1 July 2010

'What Is Cortana' (Microsoft) <<https://support.microsoft.com/en-gb/help/17214/windows-10-what-is>> accessed 9 October 2016

'What Is Do Not Track' (Future of Privacy Forum)
<<https://webcache.googleusercontent.com/search?q=cache:iR4bdoTXI9IJ:https://alaboutdnt.com/+&cd=3&hl=en&ct=clnk&gl=uk>> accessed 7 March 2017

'What Is the EU General Data Protection Regulation?' (Strategicrisk, 2015)
<<http://www.strategic-risk-global.com/what-is-the-eu-general-data-protection-regulation/1416820.article>> accessed 17 December 2015

'When Is Processing Personal Data in Your Legitimate Interests' (Slaughter and May, 2014) <<https://www.slaughterandmay.com/media/2162779/when-is-processing-personal-data-in-your-legitimate-interests.pdf>> accessed 15 March 2017

Wiewiórowski W, 'International Cooperation of Privacy and Data Protection Commissioners' (gioda, 14 October 2014) <http://www.phaedra-project.eu/wp-content/uploads/2014_10_13_phaedra_mauritius_wiewiorowski-1.pdf> accessed 10 November 2017

Wilhelm E, 'A Brief History of Safe Harbour' (iapp) <<https://webcache.googleusercontent.com/search?q=cache:tVy-pO98WA4J:https://iapp.org/resources/article/a-brief-history-of-safe-harbor/+&cd=7&hl=en&ct=clnk&gl=uk>> accessed 15 March 2018

Woodhouse J and Lang A, 'Brexit and Data Protection' (House of Commons Library, 10 October 2017) <<file:///C:/Users/User%201/Downloads/CBP-7838.pdf>> accessed 22 January 2018

'Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (Europa, 2005) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf> accessed 17 January 2016

Yates J and Arne P, 'Protecting Your Visitors: California's Online Privacy Protection Act Could Set Standards' (LocalTechWire) <https://www.mmmlaw.com/files/documents/publications/article_228.pdf> accessed 4 March 2017