Durham University

Durham E-Theses

The problems of protecting privacy and reputation online under English tort law: can "the right to be forgotten" provide the solution?

FIONA BRIMBLECOMBE

How to cite:

BRIMBLECOMBE, FIONA (2020) The problems of protecting privacy and reputation online under English tort law: can "the right to be forgotten" provide the solution? Doctoral thesis, Durham University.

Use policy

The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a https://etheses.durham.ac.uk/id/eprint/13506/ is made to the metadata record in Durham E-Theses
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Please consult the full Durham E-Theses policy for further details.

Academic Support Office, The Palatine Centre, Durham University, Stockton Road, Durham, DH1 3LE
e-mail: e-theses.admin@durham.ac.uk Tel: +44 0191 334 6107
https://etheses.durham.ac.uk

Thesis title: The problems of protecting privacy and reputation online under English tort law: can "the right to be forgotten" provide the solution?

Author: Fiona Brimblecombe

Abstract

This thesis operates around a central premise: there is a lack of personality rights for individuals in England and Wales with respect to personal information on the internet. This thesis examines whether the 'right to be forgotten' also known as the 'right to erasure' in Article 17 of the General Data Protection Regulation 2016 (GDPR) and enshrined in the Data Protection Act 2018 will begin to remedy this problem. This PhD firstly examines what the 'right to privacy' actually is by turning to legal theory – and adopts a working definition. It then moves to consider aspects of the GDPR that have relevance to the right to be forgotten and its exemptions. The thesis as a whole conducts a normative analysis through the lens of Article 8 of the European Convention on Human Rights – the right to private and family life. It draws on the breadth of Article 8 Strasbourg caselaw in order to extrapolate key 'balancing principles' which could be utilised by the English courts when interpreting the new erasure right. It also extrapolates principles from Strasbourg Article 10 (freedom of expression) caselaw, with suggestions on how these factors could be used by the courts when interpreting the right to erasure's freedom of expression and journalism exemptions. Finally, it undertakes an assessment of both the English torts of misuse of private information and defamation. It highlights their failings and their patchwork protection of reputation-rights in respect of private information online. It strives to prove that the right to be forgotten, although not a perfect solution, does provide a better route to redress with respect to personal data online than both of the English torts currently in operation.

The problems of protecting privacy and reputation online under English tort law: can "the right to be forgotten" provide the solution?

Fiona Brimblecombe

PhD Thesis (Law)

Ustinov College

Durham Law School, Durham University

2019

Table of Contents

Chapter 1: introduction……8

A. Threats to privacy in the digital age……..9

B. The newly-formulated right to be forgotten under the GDPR…….14

C. Research questions……..…17

D. The scope of this thesis……...……20

E. Original contribution to knowledge…….21

F. 'Data-leak' scenarios……23

G. Outline of the structure of this thesis……...25

H. A note on the structure of this thesis……...…29

Chapter 2: what is privacy and why should it be protected……....31

A. Searching for a theoretical definition of privacy…….31

B. Why is it important privacy is protected…….43

Chapter 3: The GDPR, the 'right to be forgotten' and Article 8 ECHR……...……..49

Part 1: Article 17 and the EU's new data protection framework…….49

A. An enhanced role for Data Protection Authorities……..50

B. Key definitions relevant to the GDPR……51

C. A respondent data controller's liability for the actions of third party controllers……...58

D. Domestic Purposes Exemption……60

E. Consent to data processing in the GDPR……65

F. Special category data……67

G. Data protection principles……73

H. What is the 'right to be forgotten'?……75

Part 2: How will Article 17 GDPR be interpreted according to Article 8 ECHR……93

A. How is the ECtHR caselaw relevant to the interpretation of a EU Regulation?.....……94

B. Scope of the chapter……96

C. A preliminary note on different data dissemination scenarios……97

D. Analysis of European Court of Human Rights Article 8 jurisprudence……100

E. The REP test and different data dissemination scenarios……...…103

F. The goals of Article 8 protection as defined by the ECtHR's reasonable expectation of privacy test in comparison to the aims of the right to be forgotten……106

G. An analysis of the ECtHR's balancing factors going to the weight of the Article 8 claim and their application to the right to be forgotten……108

Chapter 4: Strasbourg and English jurisprudence concerning freedom of expression and its application to the right to be forgotten……...132

A. Theoretical justifications for freedom of expression……132

B. Analysis of the European Court of Human Rights' Article 10 jurisprudence……...141

Chapter 5: Domestic 'privacy' law and its efficacy in protecting personal data online…...170

A. The origins of the tort of misuse of private information……...173

B. Outlining the elements of MPI; initial criticisms……..…174

C. The erratic treatment of press freedom in MPI's caselaw…….179

D. The various interpretations of the doctrine of waiver in MPI……...189

E. The notion of the information as in the 'public domain'……...196

F. Remedies in MPI……202

Chapter 6: Defamation and the dissemination of false and private information online…...225

A. Data dissemination scenarios……....228

B. Defamation at Strasbourg: reputation's protection under Article 8 ECHR……...228

C. The inadequacies of the Defamation Act 2013……..233

Overall conclusion……...…286

Bibliography……...290

Statement of Copyright

The copyright of this thesis rests with the author. No quotation from it should be published without the author's prior written consent and information derived from it should be acknowledged.

Part of this thesis (Chapter 3, part 1) has already been published in an academic article: Fiona Brimblecombe and Gavin Phillipson, 'Regaining Digital Privacy? The New 'Right to be Forgotten' and Online expression' 4(1) Canadian Journal of Comparative and Contemporary Law 1. It is in the 'second half' of the article – and was written by the author of this thesis. The first half of the article was written by Gavin Phillipson, and no part of his work is reproduced in this thesis. All of the work in this thesis is that of the author's.

All work in this thesis is accurate as of six months prior to the date of submission.

Acknowledgments

I would like to give thanks to a number of people who have supported me both emotionally and academically while I wrote this thesis. Namely my parents, my grandparents, friends and colleagues and in particular: Siu-Yin Ho, Charlotte Barker, Megan Tang, Kyle Murray, Tara Beattie, Anna Jobe, Andy Hayward, Ian Hargreaves and Joshua Sharp. I would also like to acknowledge the substantial efforts of both of my PhD supervisors, Prof. Gavin Phillipson and Prof. Helen Fenwick, whose advice has been invaluable. I am also deeply grateful for the generosity of Durham Law School in affording me a scholarship, enabling me to complete this work.

Dedication

For my late grandfather, William

Chapter 1: Introduction

This thesis is, in essence, a 'problem solving' PhD. It identifies a problem: that the protection for personal information and reputational rights online is inadequate, and considers how this problem can be solved. The standpoint this thesis adopts is that of an individual in England and Wales circa 2019 who has lost control of their personal data on the Web. It considers three different areas of law that could potentially provide redress for someone in that situation: the newly formulated 'right to be forgotten' in the General Data Protection Regulation 2016[1] (as enforced in English and Welsh law),[2] misuse of private information (hereafter 'MPI') and defamation in English tort law.

All three of these legal areas give rise to a key problem: each requires a balancing exercise to be undertaken with regards to 'personality rights' and freedom of expression. Personality rights include privacy and defamation; these are rights which are concerned with an individual's reputation as well as their honour and dignity. Personality rights can also protect one's personal data and be seen as proprietary in nature, in the sense that they protect an individual's right over their own image (either literally or figuratively). The thesis will use the caselaw of the European Court of Human Rights in Strasbourg (hereafter 'the Strasbourg Court' or 'ECtHR') on the balance to be struck between the 'right to respect for private and family life' under Article 8 and freedom of expression guaranteed under Article 10[3] as a broad normative framework that adduces 'balancing factors' or principles which govern how these conflicts can be resolved. A choice has been made to use Strasbourg jurisprudence for this framework rather than Court of Justice of the European Union (hereafter 'CJEU') caselaw due to the much more extensive caselaw available from the European Court of Human Rights. A further reason for doing so is the uncertainty with respect to the status and relevance of caselaw of the CJEU in English law due to of the UK's impending exit from the European Union. Section 6(2) and 6(3) of the EU (Withdrawal) Act 2018 states that CJEU caselaw (dated until the point of withdrawal of the UK from the EU) could have influence on

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L119/1 (27/4/2016), hereafter '*GDPR*'.
[2] Within the Data Protection Act 2018.
[3] Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950, 3 September 1953) 005 CETS (ECHR) (hereafter *'ECHR'*), Article 8, The Right to a Private and Family Life and Article 10, The Right to Freedom of Expression.

UK courts, but caselaw issued by the court after 'Brexit' *may* only continue to have influence in the future, section 6(2) stating:

> 'a court or tribunal *may* have regard to anything done on or after exit day by the European Court, another EU entity or the EU so far as it is relevant to any matter before the court or tribunal.'[4] Additionally, section 6(4) notes that in relation to retained EU law (enacted before Brexit): 'the Supreme Court is *not bound* by any retained caselaw'.[5]

This is in contrast to Strasbourg caselaw, which will have continued relevance to the decisions of English courts under the Human Rights Act 1998, especially section 2.

The conclusion that will be drawn from the analysis of this thesis is that current privacy rights for individuals over their personal information online in English law are inadequate in terms of fairly balancing the right to privacy against freedom of expression. Critically, privacy rights now need to be protected more than ever; as Mayer-Schönberger[6] has observed, the informational capacity of the Internet is continuing to expand alongside the vast amount of personal information posted to it, leaving an increasing number of data subjects at risk. Specifically, it will be submitted that the torts of defamation and misuse of private information are failing to provide adequate protection from the invasions of privacy and damage to reputation that occur routinely online. It will be argued that such laws have been presented with a challenge by the prevalence and dissemination of personal data online that they are failing to meet. Given that postulated inadequacy, this doctorate will explore the potential of the right to be forgotten to afford data subjects increased privacy protection online.

A. Threats to privacy in the digital age

[4] EU (Withdrawal) Act 2018.
[5] Ibid.
[6] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009), hereafter '*Delete*'.

This PhD has been written in order to address the rapidly growing technological landscape across the UK and other parts of the world, and the negative impact this has had on privacy rights online. Over the last two decades, internet access has changed from being a seldom seen digital phenomenon to being commonplace in households and workplaces: a survey in 2018 has shown that 89% of adults in Great Britain now use the Internet on a weekly basis.[7] Mayer-Schönberger has argued that we are now in the 'digital age'[8] – while technology continues to advance, the cost of purchasing such technology has decreased via competitive markets.[9] In addition, some services (such as search engines and social media sites) are free to use by the general public. The worldwide web, previously only accessible through a desktop computer and dial-up modem, can now be accessed through a range of devices, such as smartphones, tablets and laptops, all of which are portable. Due to this assortment of hardware and price-range, an increasing amount of internet-enabled technology is now readily available to individuals around the clock whether they are at home, at work, or anywhere else.[10] This increase in obtainable technology has filtered down to younger generations; a recent study has shown that one in ten children receive their first mobile phone by the age of five[11] and Ofcom has stated that the UK is now a 'smartphone society'.[12] Through this increase in prevalence of internet-enabled devices, citizens across England and Wales are now spending more time than ever before online[13] and this development has meant

[7] The survey also stated 70% of employed adults claimed that they have the ICT skills required for their job. See 'Internet access – households and individuals, Great Britain: 2018', Office for National Statistics, accessible at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018 (last accessed 28/12/18).

[8] See generally: *Delete*.

[9] On cursory inspection, it is possible as of December 2018 to purchase an Apple Iphone for £10 per month on a contract which also includes call time, texts and Internet access, courtesy of the Carphone Warehouse: see https://www.carphonewarehouse.com/mobiles/pay-monthly.html/?cid=PAIDSEARCH_Google_G%20-%20Non%20Postpay%20-%20Smartphones%20-%20BMM_Smartphones%20-%20Smartphone%20-%20Cheap%20-%20BMM_+smartphone%20+cheap_43700032979188061&&gclid=EAIaIQobChMIhZ6zwOvC3wIV1oTVCh272gdDEAAYASAAEgKW5vD_BwE&gclsrc=aw.ds (last accessed 29/12/18). Also see the Online Harms White Paper (April 2019) which discusses privacy-based online harms. Accessible at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf (last accessed 1/7/19).

[10] In 2015, the Guardian reported on a YouGov survey which stated that the average home in the UK owns 7.4 Internet-enabled devices. See 'Online all the time – average British household owns 7.4 internet devices', *The Guardian* (9 April 2015) accessible at: https://www.theguardian.com/technology/2015/apr/09/online-all-the-time-average-british-household-owns-74-internet-devices (last accessed 28/12/18). It seems safe to assume that since 2015 this number can have only increased.

[11] See 'Nearly one in 10 children gets first mobile phone by age five, says study' (*The Guardian*, 23 August 2013) accessible at: https://www.theguardian.com/money/2013/aug/23/children-first-mobile-age-five (last accessed 29/12/18).

[12] See Ofcom, 'The UK is now a smartphone society', reporting on technology usage in the UK, (6 August 2015) accessible at: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015 (last accessed 29/12/18).

[13] Ibid. The study showed that time spent online for adults 16 and above doubled between 2005 and 2015.

that an ever-increasing amount of private information is uploaded to the Internet. It is now very quick and easy to upload a photograph or other pieces of personal data about oneself or others to a website,[14] and this has gradually become a norm. Social media usage was at an 'all time high' at the end of 2018, with 83% of adults in the UK now operating a social media account.[15]

This increased use of social media has permeated into many different areas of life. People are uploading personal and private data to the Web in order to improve their job prospects (for example, by using LinkedIn), their sex lives (eHarmony, Tinder and Grindr) and their social and family lives (Facebook and Instagram).[16] With the exception of eHarmony, all of these sites are free and have a large amount of members – Facebook boasts a worldwide weekly usage of 2.27 billion individuals.[17] Alongside the rise of social media, the web is also now used to store valuable (and often personal) information. Usage of Apple's iCloud to back-up its hardware's content is now assumed when one purchases a device, and the Internet is now seen as a safe harbour where personal data can be stored through independent websites such as Dropbox.[18] Despite the growing prevalence of cloud-based storage systems, all sites which operate in this way are vulnerable to 'hackers' whose aim is to steal personal data. The news media has also stepped wholeheartedly into the digital era, with almost all news networks hosting an affiliated webpage which posts stories and bulletins.[19] Corporations such as BBC News have also created news 'apps' or applications, which deliver breaking news headlines directly to linked smartphones and tablets, free of charge.[20] The same is true for print-media – for example, many newspapers now host news applications which are updated on a rolling basis.[21] As digital reportage has instantaneous global reach, in the event that expression (which may include images) is promulgated which relates to a private individual, more people now than ever may access it.

[14] Ibid.
[15] Allison Battisby, 'The latest UK social media statistics for 2018' (*Avocado Social*, 2 April 2018). Accessible at: https://www.avocadosocial.com/the-latest-uk-social-media-statistics-for-2018/ (last accessed 29/12/18).
[16] See https://gb.linkedin.com/, https://www.eharmony.co.uk/, https://tinder.com/, https://www.grindr.com/, https://en-gb.facebook.com/ and https://www.instagram.com/?hl=en (last accessed 29/12/18).
[17] See 'The Top 20 Valuable Facebook Statistics – Updated December 2018' (*Zephoria Digital Marketing*, 28 November 2018) accessible at: https://zephoria.com/top-15-valuable-facebook-statistics/ (last accessed 29/12/18).
[18] See https://www.apple.com/uk/icloud/ and https://www.dropbox.com/h (last accessed 29/12/18).
[19] See for example BBC News' website: accessible at: https://www.bbc.co.uk/news (last accessed 12/9/19).
[20] See: https://www.bbc.co.uk/news/10628994 (last accessed 29/12/18).
[21] See for example: https://www.dailymail.co.uk/mobile (last accessed 29/12/18).

This combination of readily accessible and frequently used technology has meant that more personal and private information is being uploaded online than ever before. With this has come an exacerbated risk of the infringement of informational privacy and reputational rights, through third-parties viewing or accessing personal information online.[22] Users are now uploading personal information to the web at various different ages, and may wish to rescind previous disclosures of personal information as it is no longer fitting to their current life – yet in many situations, they are unable to do so as their data has travelled far and wide throughout the web and is no longer under their control. Take the situation where, for example, data subject 'Jane' has uploaded personal information to Facebook when she was a student studying at university, including pictures of raucous nights-out with house-mates. Jane, although able to delete the pictures from her own personal webpage, may have lost control over this information; other friends may have re-uploaded similar photographs who she has since lost touch with, or third-parties may have uploaded pictures of Jane to a 'meme' page online where pictures of other users are collated.[23] This information, uploaded several years ago, may be actively detrimental to her job hunt at a professional firm – as more employers than ever are now using social media during a candidate selection process.[24] The infamous case of schoolteacher Ashley Payne in 2011 illustrates this issue – Payne was sacked from her job at a school due to photos appearing on her Facebook account, depicting her holding a glass of wine and a pint of Guinness whilst holidaying in Ireland.[25] Indeed, there is now caselaw around unfair dismissal actions brought concerning 'historic tweets'.[26] An individual's privacy is also at risk through third parties (be it a news conglomerate or a private individual) uploading personal information about them to a potentially worldwide audience online. All types of information now disclosed online – and if a third party web user is so inclined they can post another's personal information to any part of the internet, no matter how intimate. Potential disclosures can range from benign to distressing. The English

[22] In particular Article 8 of the European Convention on Human Rights.
[23] See for example Unilad's Facebook page, accessible at: https://www.facebook.com/uniladmag/ (last accessed 22/7/19).
[24] See Lauren Salm, '70% of employers are snooping candidates; social media profiles' (*CareerBuilder.com*, 15 June 2017) accessible at: https://www.careerbuilder.com/advice/social-media-survey-2017 (last accessed 22/7/19).
[25] Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook' (*Daily Mail.com*, 7 February 2011) accessible at: https://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html.
[26] Stephen Simpson, 'Social media misconduct: fair dismissal over historic tweets' (*Personnel.com*, 19 January 2017) accessible at: https://www.personneltoday.com/hr/social-media-misconduct-fair-dismissal-historic-tweets/ (last accessed 22/7/19).

case of *AMP v Persons Unknown*[27] (that involved explicit photographs of a subject uploaded to the internet by an anonymous group using 'bittorrent' technology) is an example of one of the most distressing and serious cases of this nature from the point of view of the individual concerned. However, information as disclosed may appear benign when in fact it is not: images may reveal that a person was actually at a certain location at a certain time when they have told friends and family they were not, leading to the breakdown of relationships.[28] People from different cultures and personal backgrounds may also perceive different disclosures with different levels of severity; for example, if someone was a recovering alcoholic or was from a strictly observant Muslim family they may view a publicly accessible picture online of them drinking alcohol as extremely damaging to their reputation whereas someone else may not. Aside from ruining reputations, personal information online has hindered individuals' ability to 'move on' and forget; and Mayer-Schönberger has powerfully argued that the ability to put one's past behind them is crucial to one's future development.[29] Through the seemingly infinite 'memory' capabilities of the internet, people are finding that their past is coming back to haunt them.[30] It could be argued that the dam is already beginning to burst with regards to the sheer amount of personal data on the web; in 2018 a plethora of data protection breaches were reported worldwide. In that year alone, international hotel chain Marriott suffered a data breach which compromised the data of half a billion customers,[31] the 'Cambridge Analytica' scandal ensued where personal information was gathered from individuals' Facebook pages for political purposes without their approval,[32] and users of Quora, a questionnaire website, were hacked.[33]

[27] *AMP v Persons Unknown* [2011] EWHC 3454 (TCC).
[28] See for example, 'How can social media ruin a relationship' (*TheLoveQueen.com*) accessible at: https://www.thelovequeen.com/how-can-social-media-ruin-your-relationship// (last accessed 22/7/19).
[29] *Delete.*
[30] Nick Statt, 'Facebook confirms years-old messages are randomly coming back to haunt users' (*The Verge*, 26 November 2018) accessible at: https://www.theverge.com/2018/11/26/18113539/facebook-messenger-old-threads-conversations-resurfacing-no-reason and Toni Birdsong, 'Could Your Social Media History Come Back to Bite You?' (*McAffee*, 9 August 2016) accessible at: https://securingtomorrow.mcafee.com/consumer/family-safety/could-your-social-media-history-come-back-to-bite-you/ (last accessed 22/7/19).
[31] Tamlin Magee, 'The most significant UK data breaches' (*Computer World UK*, 4 December 2018) accessible at: https://www.computerworlduk.com/galleries/data/most-significant-uk-data-breaches-3662915/ (last accessed 29/12/18).
[32] See 'The Cambridge Analytica Files' (*The Guardian)* accessible at: https://www.theguardian.com/news/series/cambridge-analytica-files (last accessed 29/12/18).
[33] See 'Quora Hacked: Website Logs Out 200 Million Users', (*Computer Business Review*, 4 December 2018) accessible at: https://www.cbronline.com/news/quora-hack-100-million (last accessed 29/12/18).

The technological and sociological changes discussed above demonstrate that a fundamental societal shift has taken place in the internet age, which can be compared to the privacy-paradigm shift created by the introduction of the printing press in the early 17th Century. Academics have argued that libel and privacy rights were in part created because of the introduction of printed speech[34] and the telephoto lens[35] – both presenting an increased risk of damage to personality or reputation rights as a result of their potential to distribute personal information. When the printing press was introduced and printed material became increasingly commonplace, the law of England and Wales responded by adopting more exceptions to freedom of expression than had previously existed under Roman law.[36] Similarly, this thesis will argue that the laws of the present day must respond effectively to the societal shift to the 'internet age' that UK culture has undergone. Academics such as Solove and Mayer-Schönberger have stressed the importance of privacy concerns in the digital era and Mayer-Schönberger in particular has called for increased global regulation over private information on the Internet.[37]

B. The newly-formulated right to be forgotten under the GDPR

Advances made between 2012 and 2019 have broken new ground for the right to privacy in English and European law.[38] Two things have been happening in tandem, one related to the other: technology has continued to evolve rapidly and European law has striven to regulate personality rights alongside these changes.[39] Nowhere has the gulf between technology and regulation been more apparent than the internet, particularly with regards to user-generated content – a plethora of which is now online.[40] In 2012 the European Commission released a

[34] Van Vechten Veeder, 'The History and Theory of the Law of Defamation - I' (1903) 3(8) *Columbia Law Review* 546, 547.
[35] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1980) 4 *Harvard Law Review* 193.
[36] Veeder above, n 34 at 547.
[37] See Daniel Solove, 'Speech, Privacy and Reputation on the Internet' in Saul Levmore & Martha Nussbaum's (Eds), *The Offensive Internet* (Harvard University Press 2010) and *Delete*.
[38] The significance of this time period being: 2012, when the EU's Commission introduced the first draft of the new Data Protection Regulation and 2019, the year of the submission of this thesis (when the final draft of the Regulation is now being meaningfully implemented).
[39] Chapter 2 of this thesis defines the right to privacy as a claim or desire, to be inaccessible, linked to the exercise of personal autonomy and dignity. 'Personality rights' in the context of this thesis is used to refer to rights which protect an individual's reputation.
[40] Aside from privacy concerns, user-generated content has proved problematic in terms of copyright infringement, with individuals uploading content containing copywritten material to the web without permission or credit given to the copyright holders. The European Union are moving to tackle this problem through Article 13 of proposed Directive on copyright in the Digital Single Market [2016] COM(2016) 593 final (14/9/2016).

first draft of the General Data Protection Regulation, now known as the 'GDPR'[41] and realised in the UK in the Data Protection Act 2018. The GDPR came into force in May 2018,[42] repealing the previous 1995 Data Protection Directive[43] (and was infamously responsible for the deluge of emails sent by online companies to European citizens several months ago, asking recipients to update their 'privacy preferences').[44] This update was necessary as there are new types of data processing undertaken in 2019 that were not in existence in 1995 – drones are but one example of a modern device now commonly used to record personal information in an audio and visual format.[45] The emergence of 'revenge pornography' has led to intimate video footage being uploaded online as a form of harassment[46] and online 'hackers' are on the rise, seeking to target large organisations in order to acquire the personal data of others.[47] Social media use is now at a record high, with 79% of adults in the UK holding a Facebook account.[48] The breadth of different types of social media platform is also at a world high, ranging from picture-sharing applications such as Snapchat to commercial enterprises such as Depop, which is akin to a combination of picture-sharing platform Instagram and Ebay.[49] Technological hardware has continued to advance, an increasing amount of technological devices available on the market that are internet-enabled, making it easy to upload and share personal data instantaneously.[50]As a

[41] Proposal for a Regulation of the European Parliament and of the Council on the protection of personal data and of the free movement of such data (General Data Protection Regulation) [2012] COM(2012) 11 final (25/1/12).
[42] *GDPR*. See chapter 3.
[43] As will be discussed in more detail within chapter 3 of this thesis and 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 of the free movement of such data [1995] O.J L 281, 31, hereafter '*1995 Directive*'.
[44] Fiona Brimblecombe and Gavin Phillipson, 'Regaining Digital Privacy? The New 'Right to be Forgotten' and Online expression' 4(1) *Canadian Journal of Comparative and Contemporary Law* 1, 3 (hereafter '*Brimblecombe and Phillipson'*).
[45] The estimated value of the drone industry by 2025 is $90 million dollars. See Craig Smith, '25 Interesting Drone Facts and Statistics (2019)' (*DMR*, 25 June 2019) available at: http://expandedramblings.com/index.php/drone-statistics/ (last accessed 10/4/17) and Paul De Hert and Vagelis Papakonstantinou, 'The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals' (2012) 28(2) *Computer Law & Security Review* 130, 131.
[46] See Michael Baggs, 'Revenge porn: what to do if you're a victim' (*BBC News*, 24 January 2018) accessible at: https://www.bbc.co.uk/news/newsbeat-42780602 (last accessed 13/11/18).
[47] As of November 2018, there have been 11 reported hacking attempts across a plethora of online organisations (all of which store personal data), such as Facebook and British Airways. See 'List of Data Breaches' accessible at: https://en.wikipedia.org/wiki/List_of_data_breaches (last accessed 13/11/18).
[48] See Allison Battisby, 'Social usage largely aligned across the pond, key differences: Whatsapp, Pintrest, LinkedIn'(*Avocado Social*, 2 April 2018) accessible at: https://www.avocadosocial.com/the-latest-uk-social-media-statistics-for-2018/ (last accessed 13/11/18)
[49] See Depop.com: accessible at: https://www.depop.com/ (last accessed 13/11/18).
[50] 83% of mobile phone users within the UK in 2018 now use a 'Smartphone', capable of connecting to the web (and therefore sharing information online). See the survey at *Statista*, accessible at: https://www.statista.com/statistics/387218/market-share-of-smartphone-devices-in-the-uk/ (last accessed 13/11/18).

result, multiple different privacy settings are now accessible for online services.[51] Because of these continual and rapid advancements, the digital 'goalposts' have shifted significantly since 1995 in terms of not only how much personal data is on the web, but also what *type* of personal data. While a decade ago, the search of someone's name online may have only drawn a 'hit' from a mundane electoral roll listing, it is increasingly likely now that multiple social media platforms are now linked to a person's name, along with a plethora of personal information.

The GDPR sets out an enhanced data protection framework, which updates pre-existing data principles and contains new rights for data subjects with respect to their personal information online. It heralds a new era in privacy law. One of its most controversial rights, Article 17, the 'right to erasure' (also known as the 'right to be forgotten') allows for an individual, in certain circumstances, to require the deletion of personal information about themselves from the internet. The provision applies across the EU with potential extra-territorial impact: the CJEU in *Google v CNIL* accepting the possibility of a worldwide de-referencing order in the future.[52] The GDPR was created in order to respond to privacy concerns in the digital era, and to enhance and create new data rights for individuals. The then Deputy Vice-president of the Commission and EU Justice Commissioner, Viviane Reding, stated of the Regulation's first draft that it would bring a feeling of 'safety' to EU citizens and become an 'international standard-setter in terms of modern data protection rules', fusing together the previous patchwork quilt of guidelines under the 1995 Data Protection Directive.[53] The formalised introduction of the right to be forgotten in the GDPR was foreshadowed by the CJEU's decision in *Google Spain* in 2014, in which the CJEU ordered the removal of search results from Google linking to a website which detailed the claimant's social security debts (under

[51] The most obvious example of which is the ability to 'private' a social media account – to restrict access to the people who are allowed to view it. Facebook, Twitter, Instagram and Snapchat all have this function.
[52] See European Commission Fact Sheet, 'Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market' (28/1/15) available at; http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (last accessed 20/6/15). In very recent case C-507/17 *Google LLC v CNIL* ECLI:EU:C:2019:772 [72] and Cathryn Hopkins, 'Territorial scope in recent CJEU cases: Google v CNIL / Glawischnig-Piesczek v Facebook' (*Inforrm*, 9 November 2019) accessible at: https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/ (last accessed 13/2/20).
[53] Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (22 January 2012) available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (last accessed 29/12/18).

the auspices of the 1995 Directive).[54] This decision generated much debate from academics and practitioners alike – de Mars and O'Callaghan noting that it created a 'media frenzy' – with many suggesting that the judgment was an overstatement of the breadth of the 1995 Directive, or at the very least shed new light on its provisions.[55] The main concern of this thesis is to consider the extent to which this right, alongside – or going beyond – the English torts of misuse of private information and defamation, can help restore online privacy for an individual in England and Wales in 2019.

C. Research questions

This thesis seeks to provide answers to several research questions which will now be explained.

I. What is the 'right to informational privacy' and what does it seek to protect?

As this doctorate is arguing in favour of increased privacy rights with respect to personal information online, the question as to what constitutes the 'right to informational privacy' must be answered. Thus chapter 2 will consider theoretical definitions of this area of privacy via an overview of the copious literature on this matter. It will evaluate various definitions of informational privacy as proposed by different academics, and reach a conclusion as to the

[54] Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] W.L.R 659, hereafter '*Google Spain*'. For recent comment on this issue, see Advocate General Szpunar in Case C-507/17 *Google v CNIL*, Press Release No. 2/19 (10 January 2019), accessible at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002en.pdf (last accessed 4/4/19).

[55] Sylvia de Mars and Patrick O'Callaghan, 'Privacy and Search Engines: Forgetting or Contextualising?' 43(2) *Journal of Law and Society* 257, 257.The decision received a mainly negative reception, with some US commentators arguing that it would lead to censorship online. See for example: Daniel Solove, 'What Google Must Forget: The EU Ruling on the Right to be Forgotten' (*LinkedIn*, 13 May 2014) available at; https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten (last accessed 8/7/15). For wider reading, also see: Paul Bernal, 'Are Google intentionally overreacting to the Right to be Forgotten?' (*Inforrm*, 4 July 2014) available at; https://inforrm.wordpress.com/2014/07/04/are-google-intentionally-overreacting-to-the-right-to-be-forgotten-paul-bernal/ (last accessed 8/7/15), and Henry Farrell, 'Five key questions about the European Court of Justice's Google decision' (*The Washington Post: Monkey Cage*, 14 May 2014), Paul Bernal, 'The EU, the US and the Right to be Forgotten' in Serge Gutwirth, Ronald Leenes and Paul De Hert (Eds) *Reloading Data Protection* (Springer 2014) Chapter 4, 62, Viktor Mayer-Schönberger, 'Omission of search results is not a "right to be forgotten" or the end of Google' (*The Guardian Online*, 13 May 2014) accessible at; http://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten (last accessed 12/7/15) and and Orla Lynskey, 'Rising like a Phoenix: The "right to be forgotten" before the ECJ' (*European Law Blog*, 13 May 2014) accessible at; http://europeanlawblog.eu/?p=2351 (last accessed 9/7/15).

best working definition to be adopted for the purposes of this thesis.[56] It is important here to examine the definition of informational privacy as it is the purpose of this thesis to argue that online privacy protection is inadequate – and how broadly this criticism extends depends upon how this area of privacy is defined.[57] Chapter 2 also explores why it is important that privacy is protected.

II. Are any areas of English tort law able to effectively protect an individual's personal data rights, especially online, while balancing interests of freedom of expression?

To answer this question, this thesis will seek to ascertain whether an individual is adequately protected by English tort law when their personality rights have been infringed online. It will appraise an individual's likely success (or lack thereof) in regaining control of their personal information online or attaining a remedy for misuse of such information. Two main areas of tort law are relevant to this endeavour – defamation law, in particular its application to the public dissemination of false and damaging allegations of a personal nature, and misuse of private information as it has arisen from *Campbell v MGN*,[58] the closest that English law has to a privacy tort,[59] outside liability arising under Article 8 ECHR via the Human Rights Act against public authorities. The effectiveness of both torts, especially in relation to personal information online, will be evaluated via a normative analysis of the balance being struck between Articles 8 and 10 ECHR. In the case of this thesis' MPI chapter, a restatement of ECtHR Article 8 and 10 caselaw will not be undertaken in order to avoid repeating the analysis of this caselaw that has been conducted in chapters 3 and 4. It must be remembered that both torts of MPI and defamation have developed with reference to the Strasbourg jurisprudence, through the impact of the Human Rights Act 1998.[60]

[56] See chapter 2 of this thesis.
[57] Ibid.
[58] *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457, hereafter '*Campbell*'.
[59] See chapter 5 of this thesis.
[60] Both through the interpretive obligation placed on the courts through section 3 (to, insofar as possible, interpret legislation in a way which is compatible with the European Convention on Human Rights) and through how parliament has legislated in light of the Act, including the Defamation Act 2013. An obligation is present on the courts which is contained in section 6(1) of the Human Rights Act, that 'It is unlawful for a public authority to act in a way which is incompatible with a Convention right'. See Helen Fenwick, Gavin Phillipson and Roger Masterman (Eds) *Judicial Reasoning Under the Human Rights Act* (Cambridge University Press 2007).

III. How should the right to be forgotten be best interpreted in order to have the most effective impact for individuals asserting the right within England and Wales?

This right will have to be balanced against the competing right of freedom of expression, which is considered in detail in chapter 4. While misuse of private information was developed largely to answer to the requirements of Article 8, and the ECHR has had a long-standing influence on English defamation law,[61] no one has yet looked at how Strasbourg jurisprudence may affect the interpretation of the new right to be forgotten. The influence of Strasbourg caselaw here is especially relevant because of the interpretive obligation placed on the English courts through section 3 of the Human Rights Act 1998 and the continuing influence of the ECHR on English law. Hence a major part of this PhD's original contribution to knowledge will be to provide an extended analysis of Strasbourg caselaw under Articles 8 and 10, using this as a guide to the future interpretation of the new right to be forgotten, from a standpoint that favours enhancing informational self-determination.[62]

IV. Will the right to be forgotten lead to increased protection for individuals' privacy rights online and is it likely to provide a more effective means of protecting privacy online than tort law?

Article 17 is only one part of the GDPR, which updates the entirety of the EU's data protection regime. In order to answer this question and come to a conclusion concerning whether Article 17 will have a significant impact on the protection of privacy online, various aspects of the new data protection framework must be considered. This includes, for example, the Regulation's updated data protection 'principles'[63] and its new role for national Data Protection Authorities.[64] The combination of these changes in regime will alter the data protection landscape across Europe, and various interpretations of the new rules (and their

[61] *Derbyshire County Council v Times Newspapers and ors* [1993] AC 534.
[62] Chapter 3 of this thesis, which deals with this issue was developed and extended into an article co-authored with Gavin Phillipson: Fiona Brimblecombe and Gavin Phillipson, 'Regaining Digital Privacy? The New 'Right to be Forgotten' and Online expression' (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law* 1-66.
[63] *GDPR.*
[64] *GDPR,* Articles 51 to 67.

potential effectiveness) must be evaluated to determine how they pertain to an individual within England and Wales. The lack of effectiveness of English tort law with regards to privacy and reputation rights will be discussed in chapters 5 and 6.

D. The scope of this thesis

This PhD is not primarily theoretical in nature – rather, it seeks to use established theoretical insights in order to provide doctrinal and normative answers to the question of how to remedy the inadequacies of data-privacy rights online. It does not therefore purport to provide an original theoretical definition of privacy. It seeks in chapter 2 to identify an account of privacy from within the existing literature that it then uses as the starting point for its normative and doctrinal analysis. It also considers (in chapter 4) theoretical justifications for freedom of expression and their application to speech-privacy balancing with regards to informational privacy online. Article 17 is a new provision which holds the possibility of multiple different legal interpretations, and which has already attracted heavy-weight criticism from advocates of free expression online,[65] criticism which this thesis seeks to answer.[66]

This thesis will include an examination of MPI and defamation in order to ascertain how far pre-existing areas of English law are able to protect online reputation rights effectively. Both of these areas of law have an abundance of jurisprudence to draw upon and have been subject to important recent developments. Several significant judgments have been issued in MPI over the last few years[67] and the Defamation Act 2013 only came into force six years ago. An additional reason why Article 17, MPI and defamation have been focused upon is in order to consider the potential interaction and overlap between them. By way of example, both the right to be forgotten and defamation cover the scope of inaccurate data[68] and both can concern damage to an individual's reputation – someone may seek an erasure request because

[65] See for example Diane L Zimmerman, 'The "New" Privacy and the "Old": Is Applying the Tort Law of Privacy Like Putting High Button Shoes on the Internet?' (2012) 17 *Communications Law and Policy* 107.
[66] In turn, this thesis will also critique misuse of private information and defamation law.
[67] See especially *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26 and *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC).
[68] *Google Spain* concerned inaccurate or outdated information of a data subject (this case will be discussed in more detail in chapter 3). Defamation as a law solely concerns reputationally damaging *false* information.

of reputational harm that information published online can cause. The similarities between the right to be forgotten and misuse of private information are even more striking – both confer privacy rights, cover truthful information, can result in suppression or removal of private information,[69] and in application may focus on issues such as the conduct of the data subject themselves[70] and the intimacy of the information concerned, as well as any 'public interest' value disclosed information may contain. The public interest is a prevalent defence for the publication of private facts in MPI, and may well be relied upon by defendants on receipt of an erasure request.[71]

The notion of 'big data'[72] will not be discussed in this thesis. Big data concerns data sets which are so vast in size that information about a specific individual is not the focus of processing; rather, companies are interested in processing the data to analyse trends. Although the processing of big data can potentially infringe privacy rights, this is a problem for groups rather than individuals. Finally, as this thesis has a private law orientation, it will not discuss revenge pornography or online harassment offences.

E. Original contribution to knowledge

Currently there is no monograph concerning the ability of a person based in England or Wales to regain control over their personal data which has been published online, including a full analysis of Article 17 GDPR as well as MPI and defamation law. There is also a limited amount as yet written on Article 17 as it is part of a relatively new legal instrument. There exists a German monograph detailing the historic roots of the right to be forgotten but its approach greatly differs from that taken in this thesis.[73] It addresses the sole issue of the right to erasure and its history, whereas this research combines elements of English and European law in assessing an individual's data rights and anticipating future developments. The book also focuses on the issue on EU Fundamental Rights, whereas this work draws instead on

[69] Information can be deleted using the right to be forgotten and an injunction to stop publication can be granted through misuse of private information.
[70] This appeared to be a key issue in the first 'Google Spain' style case heard in the English courts: *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB), hereafter *'NT1 and NT2'*.
[71] Particularly as the Article 17(3)(a) contains a freedom of expression exemption.
[72] Large data-sets or statistics.
[73] Robert Fellner, *The Right to be Forgotten in the European Human Rights Regime* (GRIN Verlag GmbH 2014).

English privacy rights and the European Convention on Human Rights, which is not something covered in existing literature. Another original area that has been developed in this PhD is an evaluation of Strasbourg's (ECtHR) privacy jurisprudence and its potential impact upon the implementation of the right to be forgotten. This thesis examines the different ways that the ECtHR's 'balancing principles' in adjudicating on Article 8 ECHR claims can be used by the English and Welsh courts in order to interpret the scope of the right to erasure. This is an important and difficult issue and the author is not aware of any existing literature that considers this.

In addition, chapter 5 on common law privacy contains original research in that it considers how the right to be forgotten will be interpreted by the English courts alongside the tort of MPI, and how the development of MPI may colour the judiciary's approach to the new deletion right. It discusses the problems of applying the doctrines of 'public domain' and 'waiver' in MPI to personal information disclosed online and also whether recent MPI judgments have taken a 'pro-privacy' turn in light of the decisions of *PJS* and *Sir Cliff Richard*.[74] It further considers the shortcomings of injunctions in MPI as a remedy for information distributed online. A limited amount has also been written concerning both of these judgments (as they are both relatively new – one in 2016 and one in 2018) and the author is not aware of any papers relating to both the right to be forgotten and these specific cases. The author is aware of no monograph which compares the right to be forgotten and misuse of private information in the context of online privacy.

Chapter 6, concerning defamation, also provides a further original contribution to knowledge. It focuses upon the inadequacies of English defamation law in relation to online information, examining both the common law and the 2013 Act. It also considers how English defamation law can be used to procure the removal of statements harmful to one's reputation online via the liability of website operators under section 5 of the Defamation Act 2013. The chapter goes on to compare section 5 of the Act to the controversial judgments issued by the ECtHR in *Delfi v Estonia*, concerning the deletion of comments from a news portal.[75]

[74] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26 and *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC).
[75] *Delfi AS v Estonia*, App no 64569/09 (ECHR, 10 October 2013) and *Delfi AS v Estonia* App no 64569/09 (ECHR, 16 June 2015).

Finally, the approach of this thesis is unique in that it approaches the discussion of the above legal issues with reference to various 'data-leak' scenarios. These data-leak scenarios will be explained in the following section of this introduction.

F. Methodology

Several data-leak scenarios will be referred to in this thesis as concrete examples of the loss of online privacy that the thesis addresses. By considering how each of the three areas of law would apply to each scenario, and the strengths, weaknesses, gaps and uncertainties in each, both substantive problems and remedies will be illuminated. There are many different ways in which private information becomes publicly accessible online with varying degrees of involvement of the data subject in question. The key problem arises where private information (for example, a photograph) has been uploaded by the data subject themselves or a third party and the data subject wishes for that data to be removed. There would of course be no issue if a data subject had uploaded the information to their private social media page and could subsequently delete it whenever they chose. There is, however, an issue when a data subject *loses control over the data*, and it has been uploaded to third party sites which they cannot regulate. How private information became available online in any particular case is a crucial factor in arguments about reputation rights *over* this information; many advocates for freedom of expression argue that the more 'culpable' that a data subject is – by, for example, posting this information to a publicly accessible site voluntarily – the weaker their privacy claims are. Indeed, in MPI caselaw this is known as 'waiving' one's right to privacy.[76] The means by which personal data is made available online may also be relevant to how successful a data subject will be in exercising their right to be forgotten if the freedom of expression exemption is claimed.[77] The data scenarios are as follows:[78]

I. A third party uploads personal data about another to a website – the '*third party poster*' scenario

[76] Waiver is discussed in detail in chapter 5 of this thesis.
[77] *GDPR*, Article 17(3)(a).
[78] This is not necessarily an exhaustive list – other scenarios which are not mentioned here may be referred to. This list serves as an indicator of the most prevalent data-leak scenarios that will be discussed.

In this scenario, a data subject's private information has appeared on a publicly accessible website through the actions of a third party unilaterally uploading the data to the platform. For example, Jane becomes aware that a photograph of her has been uploaded by her friend Ivan to a social media platform – and Jane wishes to remove it. Here, Jane has had no control over this process of dissemination.

II. A data subject posts information about themselves to a restricted website – the '*restricted access*' scenario

Here, a data subject uploads the information in question about themselves to a partially restricted website – for example, a social media webpage set to 'private access' in that only approved people can view it. For example, Jane uploads a photograph of herself to her private Facebook account and that photograph is then disseminated more widely on other platforms by a third party who had initial access to it. Jane wishes to delete this photograph from the various sites it has travelled to. This would be particularly likely if the photograph was notable in some way; perhaps it depicts Jane in a drunken state and goes 'viral' or becomes a 'meme' – and Jane has been embarrassed by this unwanted and unforeseen wider disclosure and wishes to delete this data.

III. A data subject posts information about themselves to a public platform – the '*personal public disclosure*' scenario

Here a person has uploaded personal data about themselves to a widely accessible website. For example, Jane posts a photograph of herself on her public Twitter account. The photograph is then retweeted widely and posted on other websites over which she has no direct control, and she wishes to delete this information.

IV. The information in question does not solely concern the data subject – the '*mixed claims*' scenario

This scenario is not so much concerned with how the information has come to be on a website but the information itself. Here, Jane wishes to delete a photograph disseminated on a publicly accessible website over which she has no control; however this photograph depicts

not only her but other data subjects as well, who wish the photograph to remain visible. Here we have a conflict of interests.

V. A data subject has been made aware that private information about them is going to be published on a large scale and seeks to suppress this publication – the *'stop-press'* scenario

In this scenario Jane has been made aware that a large media corporation is about to run an exposé storyline concerning her private information in a forthcoming edition of their tabloid with corresponding online coverage. She wishes to halt this impending publication before it happens and the data is revealed.

VI. A data subject's 'personal information' has been revealed in online reports which are both false and reputationally damaging – the '*defamatory content*' scenario

Here Jane has come across online reports which detail factually incorrect private information about her and portray her in a negative light. She is concerned that the reports will damage her reputation – particularly due to the speed and ease with which information travels online.

Each chapter of this thesis, after it has considered the substantive area of law that it concerns, will then apply that law using some of the data-leak scenarios outlined above (with greater or lesser degrees of discussion depending on the context) and evaluate the likely outcome of a given scenario. The only exception to this will be chapter 6 concerning defamation, which will consider similar but amended versions of these scenarios more befitting to the tort which protects reputation rather than privacy rights. Conclusions will be drawn from comparing and contrasting various different outcomes from each discussed scenario in order to demonstrate whether or not the new right to be forgotten will create greater protection for Jane than other areas of pre-existing law, and the problems and inadequacies of English law as it previously stood or stands.[79]

G. Outline of the structure of the thesis

[79] Chapter 3 of this thesis (in part) focuses upon various 'factors' articulated by the European Court of Human Rights when evaluating whether an Article 8 ECHR claim should succeed – and relates these factors to claims for deletion under the right to be forgotten.

Chapter 2 will consider the main theoretical definitions of privacy, including the 'right to be let alone',[80] control-based definitions[81] and privacy as a state of 'desired in-access'.[82] Taking account of each of these definitions, the scope of each definition and their limitations will be evaluated and a working definition for the purposes of this thesis will then be adopted: *a claim or desire, for informational in-access linked to the exercise of personal autonomy and dignity*. This chapter will then move on to consider why it is important that informational privacy is protected, considering an individual's personal dignity, autonomy, relationships with others and personal growth.

Chapter 3 discusses the right to be forgotten and related aspects of the GDPR essential to understanding it, including key definitions such as what is 'data subject', 'personal data', data 'processors' and 'controllers'. In this vein, it also briefly discusses 'Special Category Data', and the updated set of 'Data Protection Principles'.[83] The chapter also considers who may be considered a 'journalist' for the purposes of the GDPR as well as the scope of the 'domestic purposes' exemption. Once Article 17 has been explained this chapter then considers the new right to be forgotten with reference to Article 8 ECHR. With respect to all three areas of law covered in this PhD,[84] this thesis will cross-apply the European Court of Human Rights' Article 8 and 10 jurisprudence as a normative framework for its analysis. Chapter 3 also includes an explanatory note on the respect in which ECtHR caselaw is relevant to a EU regulation. This contains discussion of the EU's accession to the ECHR, the inter-court comity between the ECtHR and the CJEU and the parallel rights to privacy in Article 8 ECHR and Article 7 of the Charter of Fundamental Rights of the EU.[85] This chapter will then consider the Strasbourg Court's 'reasonable expectation of privacy test' and the different ways that this test could apply to a court's interpretation of the right to be forgotten with reference to the above-mentioned data-leak scenarios. It will then evaluate in detail the ECtHR's 'balancing factors' which go to the weight of the Article 8 claim and their potential

[80] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193.
[81] See Richard Parker, 'A Definition of Privacy' (1973) 27 Rutgers Law Review 275, 276, Charles Fried, 'Privacy' (1967) 77 Yale Law Journal 475, Alan Westin, 'The Origins of Modern Claims to Privacy' in Ferdinand Schoeman (Ed) *Philosophical Dimensions of Privacy* (Cambridge University Press 1984) and Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2009) 75.
[82] Nicole Moreham, 'Privacy in the Common Law' (2005) 121 *Law Quarterly Review* 628.
[83] *GDPR*, Articles 9 and 5, respectively.
[84] Namely Article 17 GPDR, misuse of private information and defamation.
[85] Charter of Fundamental Rights of the European Union, (18/2/2000) OJ C364/3.

relevance to claims brought under Article 17. These factors include: the content of the information, the format in which the information is disclosed, prior conduct of a person as waiving their right to privacy, circumstances within which the information was obtained and personal data as relating to a public or a private location. The Strasbourg caselaw concerning each of these factors is evaluated and discussed and each factor is then applied to an individual claiming the right to be forgotten under various data-leak scenarios and conclusions are drawn as to how broadly the right to be forgotten ought to be interpreted.

Chapter 4 evaluates competing Article 10 free expression claims in Strasbourg and English jurisprudence. It will begin by examining freedom of expression theories and relates each key theory to the disclosure of personal information about an individual online. It will then, in a similar way to chapter 3, evaluate each balancing factor that the ECtHR and English courts adopt when assessing a competing free expression interest (against a privacy claim), and draw conclusions as to how these may influence erasure requests under Article 17 and Article 17(3)(a)'s freedom of expression and journalism exemptions. The over-arching factor that dictates the limits of a freedom of expression counter-claim is 'public interest' – in other words, the public's right to know certain pieces of private information. Various different 'sub-factors' will be considered under this umbrella, including the role of the press as a 'watchdog', information as giving an account of a particular mode of living, correcting false impressions, the role model argument and the right to criticise certain figures. Conclusions will be drawn from this analysis as to the scope of scenarios that would legitimately negate an erasure request.

Chapter 5 concerns the tort of MPI. MPI is the closest thing that English law has to a privacy tort so it is crucial that its effectiveness is evaluated in this PhD. This chapter makes several arguments. Firstly, compared to both defamation law and Article 17, MPI has one crucial advantage in terms of protecting privacy: the possibility of obtaining injunctive relief to prevent private information being published at all. Its efficacy in this regard will be considered via a close analysis of the recent Supreme Court decision in *PJS.*[86] Secondly, English courts have *at times* given preferential treatment to the press in MPI judgments through allowing weak freedom of expression claims to defeat competing privacy interests.

[86] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26.

The possibility that recent decisions such as *PJS* and *Sir Cliff Richard*[87] represent a general change of approach here will be carefully considered. Thirdly, problematic doctrines of 'waiver' and the 'public domain' have historically had the ability to negate strong privacy claims – these doctrines and their modern relevance will be examined. Again, Articles 8 and 10 ECHR serve as the normative backdrop here from which the efficacy of MPI is assessed. However, in contrast to both chapters above, ECtHR case law will not be substantively re-iterated in this chapter, as MPI as a tort was developed by the English courts in order to bring English law into compatibility with Article 8 ECHR (through obligations imposed by the Human Rights Act 1998).

Chapter 6, the final substantive chapter of this doctorate, concerns defamation in English private law. This chapter considers situations whereby a data subject's reputation rights are compromised by a third party disseminating information that is private but also *false* and damaging to their reputation.[88] In that context, as stated above, an amended version of the 'data-leak scenarios' is offered as an evaluative standpoint at the beginning of this chapter. The chapter begins by considering Article 8 and competing views concerning the right to reputation in the Strasbourg court. The largest section of the chapter concerns the inadequacies of the Defamation Act 2013 with regards to the reputation rights of private individuals and defamatory remarks made online. This section considers the codification into statute of the defence of fair comment (now 'honest opinion') and the *Reynolds* defence.[89] It also gives detailed consideration to section 5 of the 2013 Act which enables a data subject to action on defamatory content that has been posted online by third parties. Section 5's regulations can lead to this defamatory content being deleted or details being passed on to a claimant which enable them to take further action against a poster. This chapter finally evaluates the new 'Single publication rule' in section 8 of the Act and its impact on reputation rights.

To conclude, the 'golden thread' joining this PhD together is the premise of relative lack of data-rights over personal information online. The thesis is structured in such a way as to

[87] *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC).
[88] As the right to erasure, misuse of private information and Article 8 ECHR can protect information which is private but also true.
[89] The Defamation Act 2013, Sections 3 and 4 respectively.

answer the above research questions, and in particular to consider how someone based in England and Wales in 2019 would attempt to remove private information about themselves from the internet – and the different avenues of law they could pursue in order to do this.

H. A note on the structure of this thesis

As stated earlier, this thesis uses Strasbourg caselaw as a normative framework for its analysis and adopts a structure whereby after considering Article 8 and 10's scope with relation to privacy and expression on the web, it substantively cross-applies both to Article 17 and its freedom of expression exemption in chapters 3 and 4. It has been deemed necessary to do so because the right to be forgotten is a new, EU right – unlike MPI and defamation, it has not been drafted with one eye on the ECHR and many questions about the right's scope remain. To answer these questions is a demanding task, and one that this PhD attempts – but in order to do so, the principles of both Articles 8 and 10 must be put alongside the new right in order to explain how both will be applied within and to determine the scope of the right. Aside from additional relevant cases, ECtHR case law will not be substantively reiterated with regards to MPI and only briefly with regards to defamation in chapters 5 and 6. This is partially due to avoid repetition; a large amount of Article 8 caselaw and its 'factors' with relevance to MPI (as well as the right to be forgotten) is covered in chapter 2 of this thesis. It is also because MPI was developed in the English courts in order to bring English law into compatibility with Article 8 ECHR (through obligations imposed by the Human Rights Act 1998). As Lord Justice Buxton put it in *McKennitt v Ash*:

> '…in order to find the rules of the English law of breach of confidence we now have to look in the jurisprudence of articles 8 and 10. Those articles are now not merely of persuasive or parallel effect but, as Lord Woolf says, are the very content of the domestic tort that the English court has to enforce.'

Similarly, defamation law has been reformed (particularly via the Defamation Act 2013) to ensure compliance with Article 10 – so that reputation rights do not 'unfairly' trench on freedom of expression. For a considerable amount of time the principles arising out of Article

8 and 10 ECHR have had influence over English defamation law, most notably with regards to the introduction of the *Reynolds* defence for the publication of material in the public interest.

Chapter 2: What is 'privacy' and why should it be protected?

A. Searching for a theoretical definition of privacy

Academic legal literature is replete with many different definitions of privacy and in particular, informational privacy, which is what this thesis is focused upon. Firstly, the distinction must be drawn between describing what (informational) privacy *is* and (informational) privacy as *a claim or a right* that people should have.[90] This chapter will firstly unpack a definition of privacy – what privacy *is* or what a 'right to privacy' should entail and then consider why it ought to be protected, why individuals *ought to have* a right to privacy. In terms of privacy's definition, there is controversy surrounding its substantive content and scope. Such is the confusion that scholars such as Solove have been prompted to declare that intrusions of privacy are a 'plurality of different things that do not share one element in common'.[91] Rather than attempting to formulate an exhaustive definition of privacy, Solove instead proposes that compiling a taxonomical list of potential invasions of privacy is of more value.[92] With regards to privacy *as a right*, there is argument as to whether it is fundamentally founded in proprietary interests (intellectual property law) or is a human right, sometimes seen as related to the harm principle.[93]

Despite the difficulties in reaching a coherent definition of privacy, it is important that a working definition is established in terms of this thesis. This is because the way in which privacy is perceived will influence how the interpretation of laws impacting the *right to* privacy are evaluated in this work. Accordingly, this chapter responds to 'research question' number 1: *what is the right to privacy and what does it seek to protect?* In the first section of

[90] For example, two individuals of different backgrounds may agree on a definition of what privacy *is*, however they may fundamentally disagree over someone's *right to have it*. For example, a member of the East German Stasi may agree with a leading privacy academic over privacy's *definition*, but disagree with the academic that individuals should be afforded *the right to it.*

[91] Daniel Solove, '"I've Got Nothing to Hide" and Other Common Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745.

[92] Ibid.

[93] See Andrei Marmor, 'What is the Right to Privacy' (2014) 43(1) *Philosophy & Public Affairs* 3 (who argues that the right to privacy is proprietary), Edward Bloustein, 'Privacy, tort law, and the constitution: is Warren and Brandeis' tort petty and unconstitutional as well?' (1968) 46(5) *Texas Law Review* 611 (who notes confusion around whether in fact privacy is encompassed within intellectual property law) and David Hughes, 'Two concepts of privacy' (2015) 31 *Computer Law & Security Review* 527 (who argues that the right to privacy derives its legitimate basis from the harm done to a data subject when personal information is released about them). Also see the *ECHR*, Article 8 (the right to private and family life).

this chapter, this thesis will argue (contrary to Solove) that there are in fact several unifying factors that make up the definition of informational privacy – making it unique, distinctive and definable. Furthermore, breaches of informational privacy are commonly justified with reference to the protection of free speech. Several popular definitions of privacy will now be examined in turn and their relative merits and shortcomings evaluated, so that conclusions can be drawn towards a working definition.

I. The right to be let alone

i. Scope of the definition

It is impossible to write about the theoretical definition of privacy without mentioning Warren and Brandeis' seminal article. However, within their trailblazing piece, the pair – who were practitioners – were largely set on framing the right within US law, rather than defining it so their piece will not be discussed at length here. What remains to be said is that they describe privacy as the 'right to be let alone' and this was perhaps the most famous attempt to sketch the scope of the right to privacy within the 19th century.[94] Their piece, although falling short in terms of a definition, had merit for bringing the issue into topical discussion; their work can be viewed as forming the initial impetus for debates eventually leading to the US privacy torts defined by Prosser.[95] Warren and Brandeis' article also has value in its helpful distinction between privacy violations and defamation. The authors noted that defamation is a material wrong, altering views about the person in question in another's eyes (primarily concerned with *false and misleading* information).[96] In contrast, privacy is a wrong often concerning *truthful* personal details.[97] Warren and Brandeis also refer to the 'spiritual nature of man's being' as an aspect of privacy (and why it ought to be legally protected). This can be interpreted as a commendable, yet unelaborated, effort to relate privacy to an individual's spiritual feeling of being wronged when intruded upon while engaged in a private activity.[98]

[94] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193.
[95] However, the framing of the Prosser torts has proved contentious and ultimately lacklustre; see Edward Bloustein, 'Privacy as an aspect of human dignity: an answer to Dean Prosser' (1964) 39 *New York University Law Review* 962.
[96] The Defamation Act 2013, Section 2(1), The Truth Defence.
[97] See Bloustein above, n 95, 968.
[98] See Edward Bloustein, 'Privacy, tort law, and the constitution: is Warren and Brandeis' tort petty and unconstitutional as well?' (1968) 46(5) *Texas Law Review* 611, 612-613 who references Harry Kalvern, 'Privacy in tort law – were Warren and Brandeis Wrong?' (1996) 31 *Law & Contemporary Problems* 326.

However admirable their endeavour may have been, there are many well-known shortcomings to Warren and Brandeis' formation of privacy. Crucially, the notion of a 'right to be let alone' is left undeveloped and lacking in detail. Their article chiefly focuses upon *why* the right to privacy was necessary in the 19th Century (they believed it was necessary due to the invention of the printing press and the camera generating idle gossip) rather than defining what the right to privacy actually meant or its intended scope. Therefore, Warren and Brandeis' definition of privacy must be concluded as being broad and vague – and therefore of limited use.[99]

II. Control-based definitions of privacy

i. Scope of the definitions

A control-based definition of privacy, advocated by academics such as Fried and Westin, theorises that privacy is the ability of an individual to control the extent to which personal information about themselves is conveyed to others.[100] This particular definition of privacy is frequently relied upon in academic literature as well as caselaw.[101] Reiman notes that a fundamental facet of privacy, ensuring 'personhood' and individual autonomy, is the ability of a data subject to choose who observes them and therefore *control* who gains personal information about them.[102] Privacy–as–control is rooted within Parent's 'personal knowledge' definition of privacy, Parent stating that 'privacy is the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him.'[103] Using this reasoning, the capacity of an individual to dictate who possesses personal knowledge relating to themselves directly correlates to a positive exercise of a right to privacy.

[99] Chris Hunt, 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort' (2011) 37(1) *Queen's Law Journal* 167, 179-180.
[100] See for example: Richard Parker, 'A Definition of Privacy' (1973) 27 *Rutgers Law Review* 275, 276, Charles Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475, Alan Westin, 'The Origins of Modern Claims to Privacy' in Ferdinand Schoeman (Ed) *Philosophical Dimensions of Privacy* (Cambridge University Press 1984) and Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2009) 75.
[101] Ibid Nissenbaum and see for example Lord Hoffmann's judgment within *Campbell*, and Nicole Moreham, 'Privacy in the Common Law' (2005) 121 *Law Quarterly Review* 628, 638.
[102] Jeffrey Reiman, 'Privacy, Intimacy and Personhood' (1976) 6(1) *Philosophy & Public Affairs* 26, 37.
[103] W. A. Parent, 'Privacy, Morality and the Law' 12(4) *Philosophy & Public Affairs* 269, 269.

The crux of a control-based theory of privacy rests upon the proposition that a person should have (at least some degree) of power over the extent to which information concerning themselves is disclosed to various third parties at different times.[104] Reiman analogies this control mechanism to an outsider's view into a fishbowl - the fishbowl a metaphor for a person's personal information and the outside observer a third party. When peering into a fishbowl, only certain parts of the tank can be observed at different times, due to refraction of light rays through water.[105] Similarly, a person controlling disclosure of their private information to third parties allows them to restrict access to certain pieces of private information to certain individuals in their lives. This metaphor can be contrasted with the idea of an 'informational panopticon', a circular prison with glass walls whereby inmates are visible to outsiders at all times – the prisoners thereby having no control over their personal privacy.[106]

Fried argues that a data subject's privacy centres on their ability to restrict information about themselves, revealing differing types and amounts of information to different people in their lives. Fried believes that this restriction helps individuals in fostering different kinds of relationships with others; perhaps a person would inform his best friend of certain intimate details about his personal life, but not his mother–in–law.[107] Westin observes that individuals adopt alternating 'faces' dependent upon with whom they are interacting.[108] This is a result of social 'norms' which dictate that an individual should behave in a certain way in a particular context: for example, certain standards of behaviour are expected from parents to children or between spouses. It is often expected in modern society that a parent should present themselves to some degree as a 'role model' for their children, providing an example of a respectable way to live.[109] In order to set a good example, parents may wish to keep certain aspects of personal information relating to themselves private from their children – in other words, exercise control over the dissemination of this personal information. Jouard notes that

[104] Nissenbaum above, n 100 at 71.
[105] Ibid 75.
[106] Ibid 75.
[107] Fried above, n 100 and James Rachels, 'Why Privacy is Important' (1975) 4(4) *Philosophy & Public Affairs* 323.
[108] Westin above, n 100 at 56.
[109] Research has shown that many children perceive their parents as role models or heroes: see for example Kristin Anderson and Donna Cavallaro, 'Parents or Pop Culture? Children's Heroes and Role Models' (2002) 78(3) *Childhood Education* 161.

adhering to social norms is not an insubstantial burden imposed upon citizens in modern society.[110]

It is important to note that *full* or complete control for an individual over the dissemination of personal data relating to themselves is neither desirable nor realistic. Indeed, proponents of the 'privacy as control' definition concur that only a *degree* of control is necessary for an individual to exercise privacy rights. Nissenbaum states that there is general agreement in the legal academic community that full informational control is undesirable and impossible; for example, when we walk down a street people may observe us and in doing so gain personal information about us.[111] However, some control is still exercised here – when walking in public individuals do certain things in order to shield or 'control' access to certain aspects of themselves (or private life); for example, people wear clothes to hide their bodies when walking down a street and typically would not go to the toilet in public. Gaining complete control over all personal data would require an individual to become a recluse.[112] Shils observes that data subjects seldom desire total or complete privacy with regards to their personal data, rather the ability to limit data flow to particular individuals.[113] Marmor also presents a tempered offering of a control-based definition of privacy, suggesting that one should be given a '*reasonable* measure of control over ways in which we present ourselves to others.'[114]

ii. When personal information is voluntarily disclosed from the data subject to another

The operation of a control-based definition of privacy warrants scrutiny when applied to a situation whereby an individual voluntarily discloses personal data concerning themselves to a third party. Academics such as Moreham and Gavison believe that this type of situation reveals a flaw of a control-based definition of privacy, due to the fact that in this type of

[110] This point will be discussed in more detail in the second part of this chapter. See Sidney Jouard, 'Some Psychological Aspects of Privacy' (1966) 31 *Law & Contemporary Problems* 307.
[111] Nissenbaum above, n 100 at 73, Reiman above, n 102 at 37 and Judith Jarvis Thomson, 'The Right to Privacy' (1975) 4(4) *Philosophy & Public Affairs* 295, 311.
[112] Moreham n 101 at 639.
[113] Edward Shils, 'Privacy: its constitution and its vicissitudes' (1966) 31 *Law & Contemporary Problems* 281, 306.
[114] Andrei Marmor, 'What is the Right to Privacy' (2014) 43(1) *Philosophy & Public Affairs* 3, 14 [emphasis added].

scenario it can be argued that privacy is simultaneously both exercised and lost.[115] The privacy of a data subject is *exercised* or enjoyed in the sense that they are invoking their control over the dissemination of private data by positively choosing to disclose to whom their personal data is conveyed.[116] Conversely, it could be said that the data subject has relinquished control over their personal details by informing another of them, as the confidante may then impart the information to a third party.

In response it may be said that a person's disclosure of personal data to another does not mean that control over that data has automatically been lost. The subject has exposed themselves to the chance of that person relaying the information to someone else, therefore increasing the *risk* of some control over the data eventually being lost. If the eventuality arises that the confidante does in fact disseminate the information in question to other third parties, *then some control over the information has been lost*.[117] If a person has been highly selective about who they have disclosed information to then they have retained *some degree* of control over the information as they have only passed this information on to particular people; control has only been fully lost when information is publicly available. Similarly, control has been reduced if an elaborate technological contraption has been used to record a subject's phone calls but the operator of the contraption has not listened to the recordings. A subject here has (perhaps unknowingly) been exposed to a *risk* of loss of control over their information, but it has not yet been lost.[118]

iii. Criticisms of an *informational control*–based definition of privacy

An *informational control* based definition as opposed to a broader *control*-based definition of privacy has significant flaws, in the sense it is simplistic.[119] An *informational control* definition suggests that if no new information relating to a data subject has been gained by a third party, the subject's privacy has not been breached; as according to an informational control definition, the gravity of the privacy breach depends upon the quality and quantity of

[115] Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89(3) *The Yale Law Journal* 421, 427 and Moreham above, n 101 at 639.
[116] Parker n 100 at 295.
[117] See Thomson n 111; C/f Moreham above, n 101 at 638, Parent n 103 at 273 and Gavison above, n 115 at 427.
[118] In the digital age, surveillance in this way is not hard to imagine.
[119] Moreham above, n 101, 649-650 and Parker above, n 100 at 276.

information obtained from an intrusion.[120] If a former lover covertly observes his past girlfriend taking a shower, it could be argued according to a strict reading of an *informational control* definition of privacy that, as he already knows what his ex–girlfriend's nude body looks like, her privacy has not been violated.[121] It is submitted here that this is not the case; as Moreham notes, an informational control definition 'does not adequately explain what is obtained (or lost) when one person looks at another against his or her wishes.'[122] Bloustein terms this type of breach as an 'insult to individuality'[123] and a reduction in human dignity – an individual's autonomous preference as to who observes them has been breached, regardless of whether any new information has in fact been gained.

III. Privacy as a subjective desire for a lack of accessibility

i. Scope of the definition

Moreham advocates a definition of privacy as desired inaccessibility.[124] Framing privacy as a subjective desire for lack of personal accessibility is useful as it pertinently observes that to enjoy a right to privacy, one must *wish* to be free from other's access. This avoids the pitfall of declaring that a person stranded on a desert island is enjoying perfect privacy, regardless of the fact that they are desperate for human contact.[125]As noted earlier, Moreham argues that an individual rarely wishes for complete and total in-access to herself; rather we normally seek a *degree* of in-access, and the ability to disclose what we choose to who we choose at a particular time.[126] Viewing privacy as a desire also allows individuals to manifest their free will in choosing whether to waive their right to privacy in any given situation.[127] Moreham's definition also has merit in that it appears to take inspiration from the idea that privacy serves an important purpose in protecting human autonomy and dignity.[128] Reiman concludes that due to 'moral ownership of our bodies', citizens should be able to choose by whom they are

[120] Moreham above, n 101 at 650.
[121] See Moreham, n 101 at 650 and Parker n 100.
[122] Moreham above, n 101 at 650 and Nissenbaum above, n 100 at 70.
[123] Bloustein above, 95 at 981.
[124] Moreham above, n 101.
[125] For a differing opinion see for example Gavison above, n 115 at 431 who speaks of 'perfect privacy' as someone in total solitude, unable to be seen, heard or contacted by others; arguably she has fallen into the abovementioned 'pitfall' by not focusing upon privacy as something to be subjectively desired.
[126] Moreham above, n 101 at 637 and Shils above, n 113 at 306.
[127] Moreham above, n 101 at 637.
[128] Moreham above, n 101.

sensed, or accessed. Ensuring our autonomous choice as to this matter respects our human dignity.[129]

Nissenbaum notes that privacy as desired inaccessibility and privacy as control are two of the most prevalent definitional frameworks of the right.[130] It is submitted here that rather than viewing inaccessibility and control as separate theoretical definitions of privacy, Moreham's access-based definition should rather be viewed as a more specific conception of 'privacy as control.' Subjectively desired inaccessibility involves an individual's control over who can observe them or sense them at that particular time, regardless of whether any new information is gained in doing so, similar to privacy as control.[131] An access-based definition of privacy dictates that the seriousness of a breach is equivalent to the degree to which *control has been lost* when a person has been observed against their wishes.[132] Hunt concurs, noting that privacy through inaccessibility is concerned with controlling how a person is perceived; how they are looked at, touched or heard.[133] Rachels also analyses the overlap between a control–based definition of privacy and privacy as inaccessibility, stating: 'if we cannot control who has access to us, sometimes including and sometimes excluding various people, then we cannot control the patterns of behaviour we need to adopt or the kinds of relations with other people that we will have.'[134] Much like a control-based definition, academics argue that complete inaccessibility to an individual by others is neither practical nor desirable; rather, many believe that whether a person is experienced should not be unilaterally at the discretion of a third party.[135]

Hunt has developed a refinement of Moreham's definition of desired in-access, his definition reading:

> *privacy is a claim to be free from sensorial and informational access, importing the limiting factors of intimacy, societal context and the subjective nature of an*

[129] Reiman n 102 at 38 and Stanley Benn, 'Privacy, freedom and respect for persons' in Ferdinand Schoeman (Ed) *Philosophical Dimensions of Privacy* (Cambridge University Press 1984) 223, 226-7. This will be discussed in more detail in the second half of this chapter.
[130] Nissenbaum n 100 at 69–70.
[131] Parker above, n 100 at 280-281.
[132] Parker above, n 100 at 284.
[133] See Hunt above, n 99 and David Hughes, 'Two concepts of privacy' (2015) 31 C*omputer Law & Security Review* 527, 534.
[134] Fried and Westin both above at n 100 and Rachels n 107 at 331.
[135] Nissenbaum above, n 100 at 70.

> *individual's personality into the assessment of whether the right to privacy in a given case is legitimate.*[136]

Gerety has also previously advocated the use of intimacy as a limiting factor upon what information should be deemed private (in 1977).[137] Hunt's conception of privacy is only a partial refinement of Moreham's definition and imports two helpful factors from Moreham's version of privacy, namely privacy as a *desire* facilitated by *in-access*. His definition includes a number of limiting factors on the right to privacy (and when it can be invoked), such as the intimate value of the information, societal context in which the data is disseminated and the subjective nature of the claimant's personality; these factors utilised in evaluating the weight of the privacy claim. Hunt's definition is helpful in emphasising the importance of the subjective mind of the individual seeking to assert their privacy rights, as certain data subjects may be peculiarly sensitive to having certain facts revealed about themselves – a factor unaccounted for by many mainstream privacy definitions. For example, an individual who is a politician may wish to restrict access to even banal personal details on a social networking site such as Facebook for fear of information concerning her being observed by the public and political opponents, undermining her sense of authority and professionalism.[138]

Hunt cogently notes that societal context is another relevant factor in determining what ought to be perceived as private data. Different cultures within society may view the right to privacy concerning certain details about oneself with varying degrees of seriousness.[139] For example, pictures hosted on a social networking site of an individual drinking alcohol may not be deemed particularly significant if the individual in question is secular, whereas if the individual is a devout Muslim or Sikh such a picture may be deemed highly sensitive, and they may have a heightened wish to restrict the picture's dissemination to others.[140]

Like Hunt, Nissenbaum argues that societal context is relevant to the scope of a right to privacy. Nissenbaum states that privacy is 'neither a right to secrecy or a right to control but a

[136] Hunt above, n 99.
[137] Ibid and Tom Gerety, 'Redefining Privacy' (1977) 12(2) *Harvard Civil Rights – Civil Liberties Law Review* 233, 281.
[138] Website 'New Media Campaigns' advises political candidates to create a 'work' Facebook page and to 'hide' their personal Facebook page. Accessible at: https://www.newmediacampaigns.com/blog/10-common-mistakes-political-campaigns-make-with-facebook-pages (last accessed 23/7/19).
[139] Hunt above, n 99 at 195.
[140] Conservative readings of both the Muslim and Sikh faiths prohibit the consumption of alcohol.

right to appropriate flow of personal information.'[141] She argues that relevant societal roles, activities, norms and values contribute to whether an individual's right to privacy has been violated in a given context.[142] Post and Shils have also argued that societal feelings towards privacy rights have waxed and waned throughout history; in Medieval times, due to the small and insular nature of dwelling-places, privacy was highly valued as a method of preventing individuals revealing private details of others.[143] Shils argues that the 1960s was an era of 'deflection of attention from individuals'; instead focus was upon public political events.[144] It can be similarly argued that in contemporary culture, there has once again been a societal shift in privacy – the digital age has led to the greatest reduction in personal privacy to date due to the widespread dissemination of personal information online.[145] Technological advancements combined with the rise in popularity of social media has culminated in attention once again focusing on banal facts concerning private individuals.[146]

Hunt's definition contains certain complexities which remain unelaborated, including the methodology that is to be used when invoking the abovementioned limiting factors upon claims to privacy. His definition contains both objective and subjective elements that must be used in conjunction; the societal context of the personal data is something which ought to be objectively assessed, whereas the specific personality traits of the claimant must be subjectively analysed. Two or more limiting factors may act as counter-weights when establishing whether a right to privacy is present in a given scenario. For example, a right to privacy may be claimed, and within the relevant societal context the information disclosed may not ordinarily be seen as particularly sensitive in nature, yet, to the particular claimant, the data is particularly private. Hunt's article proffers no solution to the problem of when the objective and subjective elements of his definition collide.

The limiting factors of Hunt's definition must also be ensured as to not operate unduly narrowly, as this would unfairly restrict the amount of privacy claims deemed relevant or successful. Whether information is considered 'intimate' may be particularly susceptible to a

[141] Nissenbaum above, n 100 at 127.
[142] Nissenbaum above, n 100.
[143] Shils above, n 113 at 2093.
[144] Ibid.
[145] Daniel Solove, 'Speech, Privacy and Reputation on the Internet' in Saul Levmore and Martha Nussbaum (Eds), *The Offensive Internet* (Harvard University Press 2010).
[146] See Andrew Perrin, 'Social media usage: 2005 – 2015 – 65% of adults now use social networking sites, a nearly tenfold jump in the past decade' (*Pew Research Centre*, 8 October 2015) accessible at: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ (last accessed 14/12/15).

conservative interpretation. If someone eavesdrops upon a conversation someone has with a friend concerning exam grades or a job interview, this could be deemed a personal matter that one may only choose to share with friends, yet the topic of conversation is not intensely sensitive either, compared to a conversation about a particularly sensitive medical problem – for example, a discussion about whether someone was HIV-positive. In assessing the weight of a privacy claim under the Article 8 of European Convention on Human Rights, the Strasbourg court has expounded that the more intimate personal data is considered to be, the more likely it is to hold that Article 8 has been breached. For example, the court has held that information relating to an individual's romantic affairs will be deemed peculiarly intimate in nature, and therefore deserving of a heightened degree of privacy–related protection.[147] However, the parameters of exactly what constitutes 'intimate' data according to the ECtHR remain unclear.[148]

IV. Interim conclusions

From the above examinations of popular influential definitions of privacy, it is submitted that privacy is indeed a *subjective desire for in-access*.[149] However, this definition disregards any 'spiritual' element of the wrongdoing committed when an individual's privacy is invaded and their personality rights infringed.[150] So what then can be established as a working definition of privacy? Some tentative conclusions can be reached:

Privacy then is:

i. A claim or desire

Firstly, as earlier discussed (and encapsulated into a definition, by Moreham), privacy *is a claim or desire* to be inaccessible. It is submitted in this thesis that an individual should be in control over the degree of privacy they experience – for example, a person does not desire personal privacy with respect to their partner when having sex with them.[151]

[147] Ibid *Von Hannover (No.2)* and *Campbell*.
[148] This will be returned to in chapter 3 of this thesis.
[149] Moreham above, n 101.
[150] Ibid.
[151] Moreham above, n 101.

ii. To be inaccessible

The theoretical definitions of privacy above have established that a violation of privacy can relate to personal data about an individual as well as physical intrusions of privacy, and bodily integrity.[152]

iii. This desire for in-access is linked to an individual's exercise of personal autonomy and treatment with dignity

If an individual's desire for privacy is respected then their human dignity remains intact. Benn argues that to respect someone's privacy and solitude is to treat them as a human being, rather than selfishly observing them as if they were a specimen in a cage.[153] If people are constantly observed this reduces their autonomy of action; people behave differently if they know they are being watched, even if observation is tactful.[154]

iv. Intruding upon privacy provokes an innate reaction

This ethereal element to privacy is the innate and almost biological reaction of an individual to having their solitude being intruded upon (physically or metaphorically), as this intrusion is an 'insult to our individuality'.[155] It is submitted here that it is this aspect of privacy which makes the right unique. Moreham notes that simplistic definitions of privacy do not 'adequately explain what is obtained (or lost)' when privacy is breached.[156] This quality of privacy is independent of the nature of the intrusion, be it accidental or intentional – if an individual has been observed by another against their wishes, even without ill-intent, they have still lost this value of aloneness.[157] Furthermore, this may still be the case even if no new information is gained thereby. This feeling of affront to 'personhood' is particularly strong with regards to intrusions upon intimate situations.[158]

v. The right is subject to limiting factors

[152] Moreham above, n 101 at 648 onwards.
[153] Benn above, n 129 at 226-7.
[154] Ibid 238 and Robert Gerstein, 'Intimacy and Privacy' in Ferdinand Schoeman (Ed) *Philosophical Dimensions of Privacy* (Cambridge University Press 1984), 266, 267.
[155] Bloustein above, n 95 at 981.
[156] Moreham above, n 101 at 650.
[157] c/f Marmor above, n 114 and Thomson above, n 111.
[158] For further reading see Reiman above, n 102 and Westin above, n 100 at 64.

As discussed in relation to Hunt's definition, when privacy conflicts with high value speech, an assessment must be made as to whether privacy or expression should prevail. Certain factors can be used in order to evaluate the weight of the privacy claim. These can include (but are not limited to): the intimacy of the information concerned,[159] the societal context in which that information is made public,[160] the vulnerability or any particular personality traits of the claimant,[161] the reasonable expectation of a data subject that the information would be confidential[162] and whether the information relates to an event taking place in public.[163]

To conclude, the working definition of privacy this thesis will adopt is a claim or desire, to be inaccessible, linked to the exercise of personal autonomy and dignity. This desire may contain an innate quality of the affront to being intruded upon. When this claim to privacy collides with high value speech, the weight of the privacy claim can be assessed with reference to the factors discussed above.[164]

B. Why is it important that privacy is protected?

The previous part of this chapter sought to find a working definition of privacy for the purposes of this thesis. This section will analyse why the right to privacy ought to be protected. It is important at this point to distinguish between two different types of argument in favour of the importance of privacy. Firstly, deontological arguments are rights-based, advocating that the right to privacy has value in of itself.[165] These include arguments this thesis will endorse such as privacy as ensuring human autonomy and dignity. Secondly, consequentialist arguments centre upon privacy as a means to protect broader societal

[159] See *Von Hannover*. Also see Hunt, n 99 at 196 onwards and Gerety n 137 at 281.
[160] Hunt above, n 99 at 197-8 and Gerety above, n 137 at 238 and Robert Post, 'Three Concepts of Privacy' (2000) 89 *The Georgetown Law Journal* 2087, 2093.
[161] Hunt above, n 99 at 199.
[162] See Geoffrey Gomery, 'Whose autonomy matters? Reconciling the competing claims of privacy and freedom of expression' (2007) 27(3) *Legal Studies* 404, 410 and Althaf Marsoof, 'Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression' (2011) 19(2) *International Journal of Law and Information Technology* 110, 129.
[163] See *Von Hannover*. In chapter 3 of this thesis, these balancing factors and relevant cases will be discussed in greater detail.
[164] These are factors which will be discussed in relation to ECtHR jurisprudence in chapters 3 and 4 of this thesis.
[165] Hunt above n 99, at 203-17.

interests, such as aiding interpersonal relationships and fostering creativity – linked to the idea of 'resource privacy'.[166] The next section of this chapter will examine the most persuasive deontological and consequentialist reasons for the protection of personal privacy.

I. The protection of an individual's dignity

As stated above, privacy as ensuring human dignity is a deontological argument. Moreham and Bloustein both contend that privacy is important and necessary as it maintains one's personality and dignity rather than monetary or proprietary interests.[167] The idea of privacy as ensuring dignity and privacy as allowing for personal autonomy are often conflated, despite being two distinct legal arguments.[168] Privacy as dignity is rooted in respect for an individual as a human being, whereas privacy as autonomy enables an individual to make free life choices and construct their own personhood. Dignity is concerned with the perceptions of others, and freedom of autonomy is the wish to operate uninfluenced by others.[169] Hunt observes that the idea of privacy as ensuring dignity is a Kantian concept: an individual should be treated with due consideration rather than simply being 'used' as a means to an end by another. Dignitarian theory expounds that it is wrong for a person to watch another dressing without their approval, for example, as it disregards the subject's wishes not to be observed.[170] Benn notes that it is a fundamental 'feature of a person' to be in solitude when engaging in certain intimate activities (such as defecating).[171] The protection of privacy is therefore founded in 'respect' for another and their feelings as to their observation. The wrong emerging from covertly watching another is the fact that the outside observer does not care whether those she observes 'like it or not'.[172] Gerstein believes that to observe someone against their wishes is an inherently selfish act. The unwanted observer of an intimate activity is 'using' it in some way: perhaps satisfying their own curiosity, being entertained or even learning something new.[173] This unfairly detracts from the intimacy of the situation for those watched against their wishes. These arguments can be distinguished from Hughes' theory, which states that the wrongdoing of a privacy invasion stems from the harm that will be

[166] Hughes above n 133, at 527.
[167] Moreham above n, 101 and Bloustein above n 98.
[168] Jeffrey Rosen, 'Why Privacy Matters' (2000) 24(4) *The Wilson Quarterly* 32, 36.
[169] Post above, n 160 at 2095.
[170] Hunt above, n 99, 203-5.
[171] Benn above, n 129 at 223-4.
[172] Ibid, 231.
[173] Gerstein above, n 154 at 270.

caused by the personal information in question being made public.[174] It is submitted here that viewing privacy as dignity is a more refined argument than measuring the severity of privacy violations by the amount of 'harm' done to an individual upon the breach. The conception of privacy as dignity insists that to access a person against their wishes is to disrespect that individual, and therefore to treat them as less of a person.

II. Allowing individuals to conduct their lives autonomously

Another powerful deontological argument in favour of the protection of privacy is that it facilitates individuals in conducting their lives autonomously and allows for personal authenticity.[175] It is important that individual autonomy is maintained in order that people may construct their own sense of personal identity and are free to 'define themselves.'[176] Chlapowski submits that if private information about an individual is publicly disseminated, this can alter the way society views (and therefore treats) a person, negating that individual's ability to construct their own sense of being.[177] Westin notes that humans are keen to observe (as well as criticise) the behaviour of others as they are curious as to another's life choices. If an individual discovers information concerning another's private affairs, this facilitates the individual in evaluating their own life against that of the other person's.[178] However, it is this watchful eye and subsequent judgement which can lead to those observed feeling oppressed. This 'censorious gaze' may lead to data subjects constraining their life choices to avoid criticism, leading to a reduction in personal autonomy. If individuals are to behave freely and authentically when making life choices, particularly intimate ones, their privacy must be respected.[179] Gerstein aptly notes that people experience intimate events differently if they know another is observing; he comments, 'there is a great difference between the way we experience our own actions when we intend them to be observed and understood by others and the way we relate to them when we are immersed in intimacy.'[180] Gerstein persuasively argues that when individuals indulge in intimate activities under observation, they place themselves in the mind-set of the third party observer rather than emotionally engaging with

[174] Hughes above, n 133 at 534.
[175] Bloustein above, n 98 and Moreham above, n 101.
[176] Post above, n 160 at 2092.
[177] Francis Chlapowski, 'The Constitutional Protection of Informational Privacy' (1991) 71 *Boston University Law Review* 133, 154.
[178] Westin above, n 100 at 68.
[179] Gerstein above n 154 at 267 and Benn above n 129, at 228.
[180] Ibid Gerstein at 267.

the intimate act in question.[181]This reduces the enjoyment of the act for an individual and influences their behaviour – therefore restricting their autonomy.

III. Allowing individuals to foster healthy relationships with others

This is a consequentialist argument invoked by Rachels and Fried.[182] Rachels believes that the right to privacy is a crucial aspect of facilitating different types of personal relationships individuals have in their lives. Privacy allows a person to disclose only information that they feel appropriate to different people at different times – someone may wish to confide in their best friend or sibling about a quarrel they have had with their spouse, but perhaps not their boss at work.[183] The authors note that it is a normal part of human behaviour for individuals to choose to keep certain details private from others – and conversely, to allow others to be party to sensitive information. Gerstein, Rosen and Rachels note that this practice is not dishonest, rather a maintenance of 'moral capital.' It is human instinct to disclose intimate information to only those whose 'business [it is] to know.'[184] The expectation upon individuals to behave in a particular way when in the company of different people (playing alternate roles in an individual's life) and to adhere to standards of behaviour is a societal expectation.[185] Jouard observes that individuals comply with set patterns of disclosure through fear of sanctions or being called 'mad'.[186]

The ability to engage in emotionally intimate situations with others in private can strengthen the bond between the individuals concerned. Privacy in this sense allows a person to feel free to express their honest sentiments and behave authentically without the watchful judgement of a third party.[187] It would appear difficult for certain relationships - including sexual and romantic ones – to exist in a meaningful way without privacy for such intimate moments. A lack of public intrusion upon certain relationships (such as that of couples or parents and children) is necessary to foster closeness and an exclusivity of relationship between the

[181] Ibid Gerstein at 267-8.
[182] Fried above n 100.
[183] Rachels above n 107 at 329.
[184] Quotation from Gerstein n 154 at 266 and Rachels above, n 107 at 331 and Rosen above, n 168 at 36.
[185] Benn above, n 129 at 241, Jouard above, n 110 and Westin above, n 100 at 63.
[186] Shils above, n 113 at 308.
[187] Rachels above, n 107 at 330 and Hunt, n 99 at 125-6.

individuals involved. Indeed, Benn argues that such relationships would be destroyed without the protection of some degree of privacy. [188]

IV. Encouraging creativity and personal growth

Another persuasive consequentialist argument for the protection of privacy is that the right enables individuals to make mistakes in solitude, free of ridicule.[189] If people believed that their mistakes would be public knowledge then it is likely that the majority of individuals would feel less at ease to experiment, afraid of the mockery of others if such an experiment were to fail. Privacy therefore encourages inventiveness and creativity. Being alone in solitude also allows individuals time and space to meaningfully reflect.[190] This lends itself to a progression in the overall knowledge of society as individuals (as a result) may be able to offer enhanced cultural and economic contributions.[191] In a related matter, if a modicum of privacy is guaranteed, then talented individuals may feel increasingly inclined to take up a position of public office. If such an individual could feel sure that their private and family life would remain (to some extent) restricted from the public eye when present in such an office, their reservations about taking up such a post may diminish.[192] This would also be advantageous to society at large, as the general population benefits if gifted individuals are encouraged to adopt important public roles – as this can lead to better governance.

Cohen argues in this vein that 'privacy has an image problem'.[193] She argues that in modern times, protecting privacy has been seen as unpopular as arguments for and against privacy are too reductionist; that one must either 'support' privacy and data protection *or* technological innovation; as, she argues, there is the misconception that privacy rights hamper innovation and technology.[194] She contends that this is false – that privacy is a value that underpins 'the

[188] Benn above, n 129 at 236.
[189] Gavison above, n 115.
[190] Rosen, n 168 at 38.
[191] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015).
[192] Due to lack of privacy laws in the UK, politician Chuka Umunna withdrew himself from the Labour party leadership contest in 2015 due to fears concerning his family's lack of personal privacy (media attention had been focusing upon Umunna as a front-running candidate). See Frances Perraduin and Rowena Mason, 'Chuka Umunna withdraws from Labour leadership contest' (*The Guardian Online,* 15 May 2015) at: http://www.theguardian.com/politics/2015/may/15/chuka-umunna-withdraws-from-labour-leadership-contest (last accessed 15/12/15).
[193] Julie Cohen, 'What Privacy is For' (2013) 126 *Harvard Law Review* 1904.
[194] Ibid 1918-1919.

'liberal democracy'[195] which gives individuals the space and freedom to innovate, in a way which a society under constant surveillance does not.[196] Cohen powerfully argues that privacy allows people 'breathing room' which is what innovation needs to thrive;[197] people need to have the space to experiment with new ideas away from the scrutiny present in Orwell's Nineteen Eighty-Four.[198] She calls a surveillance society a 'modularized' society and notes that this discourages innovation – data as gathered and continually collected about individuals gives feedback which encourages predictability, rather than people with individual and novel ideas.[199]

Conclusion

There are several persuasive arguments in favour of the robust protection of privacy. These include deontological arguments of privacy as respecting human dignity and autonomy of action as well as practical and consequentialist arguments of privacy as facilitating human relationships and fostering creativity. It should be noted that the abovementioned reasons for the protection of privacy are by no means an exhaustive list – rather the above discussion attempted to gather together the most salient justifications.

The working definition of privacy reached in part one of this chapter is that of privacy as a state of desired in-access with regards to personal information. Privacy rights must be subject to certain limiting factors in the event that they collide with high value speech. Such limiting factors can include: the intimacy of the personal data exposed, the social context, vulnerabilities or particular characteristics of the claimant, whether there was a reasonable expectation of privacy and whether the information in question relates to a matter taking place within the public domain. To briefly summarise the key reasons that privacy ought to be protected, it can be stated that privacy has value as it ensures personal autonomy and dignity, as well as facilitating personal growth and different types of human relationships.

[195] Ibid 1919.
[196] Ibid 1917-1919.
[197] Ibid 1919-1920.
[198] George Orwell, *Nineteen Eighty-four* (Penguin Classics 2004).
[199] Cohen n 193 at 1917-1918 and 1927.

Chapter 3: The GDPR, the 'right to be forgotten' and Article 8 ECHR

Part 1: Article 17 and the EU's new data protection framework

Introduction

The first part of this chapter ('Part 1') will introduce aspects of the EU's General Data Protection Regulation 2016[200] (hereafter 'GDPR')[201]relevant to the interpretation of Article 17. It will also discuss the Regulation's updated 'data protection principles' and some of its exemptions – namely the journalistic exemption,[202] and the bearing both may have on the new right to be forgotten. Once the new right and data protection fundamentals have been explained, this chapter will move to discuss Article 17 with reference to the Article 8 caselaw of the ECtHR, using this as a normative backdrop for its assessment of the potential scope of the right. This second section of the chapter, Part 2, will extrapolate certain 'balancing factors' used by the Strasbourg court to assesses the strength of an Article 8 claim, and cross-apply them in order to come to conclusions regarding the scope of Article 17 and how it ought to be best interpreted to ensure informational privacy. In this sense, this chapter responds to research question III as stated in the introduction: *how should the 'right to be forgotten' be best interpreted in order to have the most effective impact for individuals asserting the right within the England and Wales?*

The GDPR succeeds the 1995 Data Protection Directive more than 27 years after its adoption. Within this time, the Directive had become out-dated due to significant advances in technology[203] and the GDPR was primarily proposed because of the perception of the Directive as obsolete. At the time the Directive was drafted, data processing and manipulation online was viewed as 'finite, traceable and identifiable.'[204] In contrast, due to the huge increase in information uploaded online and in the number of companies who utilise

[200] *GDPR*.
[201] *1995 Directive* and specifically the UK's piece of implementing legislation, the Data Protection Act 1998.
[202] Otherwise known as 'special purposes' exemption.
[203] Luiz Costa and Yves Poullet, 'Privacy and the Regulation of 2012' (2012) 28 *Computer Law & Security Review* 254, 254 and Daniel Solove, 'Speech, Privacy and Reputation on the Internet' in Saul Levmore & Martha Nussbaum's (Eds), *The Offensive Internet* (Harvard University Press 2010) 17.
[204] Paul De Hert and Vagelis Papakonstantinou, 'The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals' (2012) 28(2*) Computer Law & Security Review* 130, 131.

and store data, it is increasingly difficult to establish who truly 'controls' personal data.[205] Hard questions must be asked as to who is accountable for personal data as it appears online and who should fairly shoulder the responsibility of deleting it. The GDPR attempts to answer some of these questions (and pose new ones). It cannot be doubted that the EU Commission took a bold step in seeking to draft a Regulation containing new personal data rights to be implemented across the Union. This part of the chapter will examine the new erasure right as well as discuss other data rights and principles within the GDPR which may have an impact on how effective Article 17 is in practice.

A. An enhanced role for Data Protection Authorities

The role of national data protection 'Authorities' has been reformulated by the GDPR in an effort to overcome problems with implementation such Authorities have faced under the 1995 Directive. David Erdos recently assessed a number of Authorities across Europe (implementing the 1995 Directive's Data Protection Framework) in order to gauge how the organisations would respond to potential data protection breaches. The results of the survey indicated that the majority of national Authorities believed that data protection rules could (theoretically) apply to many situations whereby personal data is disseminated in an openly accessible manner online, in particular to social networking sites and search engines.[206] Despite this finding, the results of the survey also showed that *little actual enforcement* of data protection rules had been undertaken by the majority of Authorities against 'data controllers'; Erdos observed that there seemed to be a lacuna between the Authorities' beliefs and their 'practical reality.'[207] Such lack of enforcement indicates inefficiencies in how Authorities have functioned and Erdos has also written that there is significant variation in practice between how different national Data Protection Authorities have been operating.[208] Brimblecombe and Phillipson found that the UK's Authority had the most 'lax' attitude towards data privacy - it treated all use of social media by private individuals in

[205] Ibid 181.
[206] David Erdos, 'European Data Protection and Online New Media: Mind the Enforcement Gap' (2016) 43(4) *Journal of Law and Society* 534, 545 and 551.
[207] Ibid 552-553.
[208] Ibid and *Brimblecombe and Phillipson*, 28 and David Erdos, "Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication" (2017) 33:3 *Computer Law and Security Review* 275, 276.

disseminating the personal data of others as falling outside of the Data Protection Act 1998 - other Data Protection Authorities across Europe (in contrast) found that, when disseminated to a large or undefinable group, this would be covered under the 1995 Directive.[209]

In a bid to combat the variations in approach of national Authorities and a lack of rule-enforcement, the GDPR has introduced a more significant role for Authorities under Articles 51 to 67 of the new framework, including enhanced powers.[210] Emphasis is placed in the Regulation on the importance of rule enforcement as well as co-operation[211] between different national Authorities.[212] Article 62 of the Regulation sets out a mechanism for the 'joint operations' of national Authorities, Article 61 imposes responsibilities on Authorities to mutually assist one another during investigations and Article 63 emphasises the importance of 'consistency' between the actions of Authorities.[213] Article 68 of the Regulation creates the European Data Protection Board that will now act as a head arbiter, issuing (non-binding but influential) opinions on pivotal decisions to be made by national Authorities and promote harmonisation.[214] Such increased cohesion between decisions of national Authorities in addition to a powerful overarching Board may help give Data Protection Authorities the confidence to robustly enforce the new data protection rules against web giants.

B. Key definitions relevant to the GDPR

Definitional clarity is of utmost importance to the interpretation of data protection rules – indeed, definitions have a direct impact on whether legal instruments are interpreted broadly or narrowly. Fierce debate was engaged in by academics as well as the CJEU in the case of *Google Spain* on definitional issues such as the scope of 'consent' to processing and what

[209] See the below 'domestic purposes exemption' section of this chapter where this will be discussed in more detail and *Brimblecombe and Phillipson*.
[210] De Hert and Papakonstantinou above, n 204, 138
[211] Erdos above n 206 at 560.
[212] Costa and Poullet above, n 203 at 255.
[213] *GDPR*.
[214] *GDPR*, Article 64, also see Costa and Poullet above, n 203 at 255 and De Hert and Papakonstantinou above, n 204 at 190.

constitutes a 'data controller' under the 1995 Directive.[215] Article 4 of the GDPR contains brief definitions of key terms in the new Regulation, such as what constitutes a data controller, processor and personal data.[216] The next section of this chapter will examine these and propose particular interpretations of terms with a view to enhancing privacy online.

I. What is a 'data subject' and 'personal data'?

The definitions of both a 'data subject' and 'personal data' are crucial for the interpretation of Article 17 of the GDPR, as this mechanism applies to a deletion request by a *data subject* regarding *personal data*.[217] Article 4(1) of the GDPR defines personal data as:

> '…any information relating to an identified or **identifiable natural person** ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, **online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identit**y** of that person…'[218]

Recital 26 of the Regulation elaborates upon the definition of an identifiable natural person:

> 'account should be taken of all the means **reasonably likely to be used,** such as singling out, either by the controller or *by another person* to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the **costs of and the amount of time required for identification, taking into**

[215] In relation to consent to processing, concern was raised in particular with regards to the processing of data concerning medical treatment and whether such consent is active or passive. See for example, Sheila AM McLean (Ed) *First, Do No Harm: Law, Ethics and Heathcare* (Ashgate 2006) and David Townend, Segolene Rouille Mirza, Deryck Beylveld and Jessica Wright (Eds), *The Data Protection Directive and Medical Research Across Europe* (Ashgate 2005). Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] W.L.R 659, hereafter *'Google Spain'* held that search engines such as Google can be considered 'data controllers'. This case will be discussed later on in this chapter.
[216] *GDPR*, Article 4.
[217] *GDPR*, Article 17(1).
[218] *GDPR*, Article 4(1) [emphasis added].

> **consideration the available technology at the time of the processing and technological developments**.'[219]

These definitions are very similar to those contained within the 1995 Directive, as its Article 2(a) previously referred to personal data as relating to an 'identifiable natural person' and that account should be taken of the likely means used to identify an individual.[220] However, a small difference is the introduction of the 'likelihood of identification' criteria in Recital 26 (see above).[221] It is unclear whether this will support online privacy rights or work to their detriment. If it is interpreted in a generous manner, then it will not act as a barrier against privacy–related protection: technological developments have advanced significantly since 1995 and, as discussed earlier in chapter 1,[222] it is increasingly easy to search for and find private details about specific individuals online. This is in particular due to the increased accuracy of search engine results and 'search bar' features on social media websites as well as the option to 'tag' a third party into a photograph.[223] Given that such factors are referred to in the last part of the Recital, this would support a broad reading of what could be considered data relating to 'an identifiable natural person' online. A further new inclusion in the GDPR is the notion of an 'online identifier' as evidence which could render data personal.[224] This is a welcome introduction and demonstrates insight by the Commission that technology has evolved to a stage where it is now common to trace an internet user utilising their IP address.[225] Poullet and Costa have observed that the 1995 Directive's definition of personal data is unhelpful in 2019 as it had a preoccupation with normative identity in the form of names and address, registration numbers and healthcare data. Individuals are now identifiable by their use of a particular online application, protocol or 'cookies' online; it is no longer necessary for a data controller to associate information with a name in order to locate a person.[226] This contemporary approach of the GDPR may have the effect of enhancing online

---

[219] *GDPR*, Recital 26 [emphasis added].
[220] *1995 Directive*, Article 2(a) and Recital 26. Mark J Taylor, 'Data Protection: Too Personal to Protect?' (2006) 3(1) *SCRIPT-ed* 72, 75 and De Hert and Papakonstantinou above, n 204 at 183.
[221] *GDPR.*
[222] See chapter 1, the introduction.
[223] Facebook and Instagram in particular support this function. Facebook also supports a function whereby 'tags' are suggested to users. See Facebook Help Centre, 'Tagging Photos' available at: https://en-gb.facebook.com/help/463455293673370?helpref=faq_content (last accessed 20/4/17) and Instagram Help Centre, 'How do I tag people in my photo?' available at: https://help.instagram.com/174635396025538?helpref=uf_permalink (last accessed 20/4/17).
[224] *GDPR*, Article 4(1).
[225] See Davinia Brennan, 'GDPR series: personal data – an expanding concept' (2016) *Privacy & Data Protection* 12, 13. Also see Case C-582/14 *Breyer v Germany* [2016] (ECJ) ECLI:EU:C:2016:779, accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582 (last accessed 6/4/19).
[226] Costa and Poullet above, n 203 at 255.

privacy, as its progressive approach expands the range of data that could be considered personal by association (and therefore allows a greater range of data subjects to access the GDPR's rights).

In both the GDPR and the 1995 Directive that came before it, a key issue is and was the ability for a 'data controller' or *any other person* to recognise a data subject through personal data.[227] This is in contrast to the former definition under the UK's Data Protection Act 1998[228] which does not note the importance of a data subject's identification by an internet user: rather, only their identification by a controller is considered. Section 1(1) states:

> '"personal data" means data which relate to a living individual who can be identified—
>
> (a)from those data, or
>
> (b)from those data and other information which is in the possession of, or is likely to come into the possession of, the **data controller'**[229]

Ausloos has noted that the cases of *Breyer* and *Peter Novak v Data Protection Commissioner* have given instruction in this regard; he states 'it is also worth mentioning that there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person.'[230]

This chapter will now move to discuss the distinction within the GDPR between a data controller and a data processor. A data controller is generally construed as having more authority than a data processor – as they *control* how data is used and processed. In terms of this thesis, this distinction is crucial as it is a *data controller* who is ordered to delete

[227] *GDPR*, Recital 26 and *1995 Directive*, Recital 26. Jef Ausloos has noted that Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] (ECJ) ECLI:EU:C:2014:2428 accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212 (last accessed 17/5/19) considers a camera image of another as potentially 'personal data' [22]. See Jef Ausloos, *The Right to Erasure: safeguard for informational self-determination in a digital society?* (PhD thesis, KU Leuven, September 2018) copy on file with author.

[228] Section 1(1) Data Protection Act 1998.

[229] Ibid [emphasis added].

[230] Taylor above, n 220 at 79, and *Breyer* above, n 225 [43] and C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994 [31]. Also see Jef Ausloos, *The Right to Erasure: safeguard for informational self-determination in a digital society?* (PhD thesis, KU Leuven, September 2018) copy on file with author, 108.

information on receipt of a successful request under Article 17 GDPR.[231]

II. Who is a data 'processor'?

Article 4 of the Regulation provides that a 'processor' means a natural or legal person, public authority, agency or other body which *processes personal data on behalf of the controller*.'[232] Therefore to understand who or what a data processor is in terms of the GDPR, one must turn to the definition of data processing. According to Article 4(2), data processing is:

> '…any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, *use, disclosure by transmission, dissemination or otherwise making available*, alignment or combination, restriction, erasure or destruction;'[233]

Article 4(2)'s description of processing is comprehensive, including a large amount of different types of processing activity as well as a clause that processing can be automated (or not). This list of different processing functions would appear to include the activity of social media websites as they engage in the 'organisation' and 'dissemination' of personal data uploaded to their platform; the host formulates what a user's web homepage looks like by ordering information in a particular way and helps disseminate personal data by displaying it on a webpage. Under all of the data-leak scenarios discussed in this thesis' introduction, such a web-host could potentially therefore be liable under the GDPR for processing incompatible with the new rules.[234] These definitions of data processors and processing are closely aligned to those within Article 2 of the 1995 Directive,[235] which was found by the CJEU to include the activities of search engines.[236] The Regulation's definition would also seem to encompass third parties posting the personal information of another to a publicly accessible webpage as

[231] *GDPR*, Article 17(1).
[232] *GDPR*, Article 4(8) [emphasis added].
[233] *GDPR*, Article 4(2) [emphasis added].
[234] See Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] (ECJ) ECLI:EU:C:2018:388, accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210 (last accessed 6/4/19).
[235] *1995 Directive*, Article 2 (b) and (e).
[236] *Google Spain.*

described in the '*third party poster'* data-leak scenario as this would likely be covered under 'use, disclosure by transmission, dissemination or otherwise making available [of personal data]'.

III. What is a 'data controller'?

According to the GDPR, a data controller is:

> 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'[237]

This definition is identical to that used in the 1995 Directive.[238] Indeed, the Directive's definition of 'controller' and whether it applied to search engines was a point of contention in CJEU caselaw, particularly in *Google Spain*.[239] Advocate-General Jääskinen's opinion of the case was that although search engines processed personal data, they were not data controllers, as they did not directly control information appearing on third party sites; their function is solely to list search results. Despite his findings, the CJEU reasoned that search engines *were* data controllers; this was to ensure that data subjects would have a remedy against search-engine results as listed which contained links to pages containing personal data about them. Due to the Directive's freedom of expression exemptions it was difficult for a data subject to enforce their data rights against the *publishers* of the sites concerned, however the CJEU in finding search engines to be controllers allowed data protection rules to be levied against the likes of Google (forcing them to delist results) – providing data subjects with redress.[240] In subsequent cases across Europe, Google has acknowledged that it is in fact a data controller, such as in the English case of *NT1 and NT2 v Google*.[241] From developments in how the GDPR has unfolded to date, it appears clear that social networking website 'hosts' will be deemed data controllers for third party content posted to their websites. Recital 18 of the GDPR noting that 'this Regulation applies to controllers or processors which provide the

[237] *GDPR*, Article 4(7).
[238] *1995 Directive*, Article 2(d).
[239] *Google Spain.*
[240] *Google Spain*, [85].
[241] *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB) (hereafter known and '*NT1 and NT2*').

means for processing personal data'[242] seems to make this clear, as does a German case brought to the CJEU in 2018. The case, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, concluded that a national Data Protection Authority[243] could take action against the administrators of a Facebook page *as well as Facebook itself* as both were data controllers.[244] Although this case was decided with reference to the 1995 Directive, it will have pivotal importance for the GDPR, as the definition of data controller has remained the same. The case turned on the issue that neither the administrators of the Facebook page in question nor Facebook informed visitors to the page that personal data was being obtained from them using 'cookies'.[245] The CJEU found unequivocally that:

> 'it is not disputed in the present case that the American company Facebook and, for the EU, its Irish subsidiary Facebook Ireland must be regarded as 'controllers' responsible for processing the personal data of Facebook users and persons visiting the fan pages hosted on Facebook. **Those companies primarily determine the purposes and means of processing that data**.
>
> Next, the Court finds that an administrator such as Wirtschaftsakademie must be regarded as a **controller jointly responsible**, within the EU, with Facebook Ireland for the processing of that data.'[246]

This decision is consistent with guidance that was issued by Article 29 Data Protection Working Party[247] in 2010 which states that in circumstances where there are multiple issues of 'control' over personal data that *joint and several liability* as controllers should be enforced on the relevant parties.[248] Article 29 Working Party have noted that it was initially

---

[242] *GDPR* and *Brimblecombe and Phillipson*, 31.
[243] Data Protection Authorities and their roles are discussed below.
[244] More specifically, the Facebook devolved 'subsidiary'. See Case C-210/16 *Unabhängiges* above, n 234 and also see Court of Justice of the European Union – Press Release No. 81/18 (Luxembourg, 8 June 2018),'The administrator of a fan page on Facebook is jointly responsible with Facebook for the processing of data of visitors to the page' accessible at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081en.pdf (last accessed 11/3/19).
[245] Ibid *Press Release*, at 1.
[246] Ibid *Press Release*, at 2 [emphasis added].
[247] Article 29 Data Protection Working Party was an important body that existed from 1995 up until the enforcement of the GDPR which was made up of a representative from each *national data protection authority* of the EU which issued guidance on privacy and data protection regulation. It was independent and had an advisory capacity. See: https://edpb.europa.eu/our-work-tools/article-29-working-party_en (last accessed 26/7/19).
[248] Article 29 Working Party here uses a myriad of different examples to illustrate their point. See Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (adopted 16 February 2010),

the European Commission's suggestion to hold multiple data controllers (pursuant to the same data) jointly and severally liable 'so as to protect the natural persons about whom the data are processed'.[249] They also noted that in the case of joint controllers, 'the participation of the parties to the joint determination may take different forms and does not need to be equally shared' in order for joint and several liability to be incurred.[250] For the purpose of this thesis, this would mean that a *third party poster* of another's personal data and a *social media website* who hosts the information could both be jointly and severally liable as controllers – despite the fact that both parties are fulfilling very different functions.[251]

A past question that has been raised by Keller[252] is whether finding social media websites responsible as data controllers would conflict with the E-Commerce Directive, as the Directive acts to shield host websites from liability for the content uploaded onto their platforms if a host has no knowledge of it as illegal.[253] In response to this query, Erdos states that as the GDPR's right to be forgotten does not require websites to *continually monitor* their sites for certain content, he believes that this does not conflict with the E-Commerce Directive.[254] Article 17 is a remedy with a retroactive effect, and for information to be deleted, this must be first be requested by a data subject.

C. A respondent data controller's liability for the actions of third party controllers

As first proposed in 2012, Article 17(2) of the GDPR contained a provision whereby an 'initial' data controller who 'has made the personal data public' was responsible for taking

---

accessible at: https://www.pdpjournals.com/docs/88016.pdf (last accessed 11/3/19) 7-24. Also see *Brimblecombe and Phillipson*, 31.

[249] Ibid Article 29 Working Party, 17-18.

[250] Ibid 19.

[251] Ibid 21.

[252] Ibid *Brimblecombe and Phillipson* and Daphne Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation', *Social Sciences Research Network* (22 March 2017), accessible online at: https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2914684 (last accessed 11/3/19).

[253] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2008] OJ, L-178.

[254] *Brimblecombe and Phillipson*, 32 and see David Erdos, 'Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU *acquis*' (2018) *International Journal of Law and Information Technology* 189, 217.

'reasonable steps' to contact third party controllers and processors to inform them of an erasure request.[255] Such controllers could also be held responsible for subsequent republication of personal data, if they authorised it – on the basis of strict liability.[256] These provisions were diluted in Article 17(2)'s final formation from its progression through the European Parliament. It no longer contains a provision whereby controllers are liable for subsequent republication and a caveat has been added to clarify what constitutes 'reasonable steps':

> '…taking account of available technology and the cost of implementation…'[257]

This may work to negate the liability of controllers to contact third parties if the costs to do so are onerous. This could be the case where the third party has made an anonymous account with the social media site in question (that the controller operates), and it is difficult if not impossible to contact or trace them – as technology or time constraints prohibit this. The caveat appears to create a 'middle ground' between mitigating seemingly punitive strict liability upon data controllers and including an accountability measure to give redress to data subjects whose data has been posted across multiple sites. This was perhaps an inevitable consequence of Article 17's subsequent redrafts, subject as it was to strong criticism on the grounds of infringing freedom of expression and hindering the operation of big business.[258] It is argued here that this addition should not be interpreted in an unduly broad manner, in the sense that any or even moderate expenditure required by an 'initial controller' in contacting a third party would negate their liability to contact subsequent controllers. This would lead to a situation where a data subject would be able request erasure from one website, but would not have aid in notifying other controllers from sites where that information has been further disseminated to. Often this further dissemination is the most damaging aspect of publicly available information (data can spread far and wide after becoming popular or going 'viral')[259] and it would be difficult financially and temporally for a private individual to take

[255] Proposal for a Regulation of the European Parliament and of the Council on the protection of personal data and of the free movement of such data (General Data Protection Regulation) [2012] COM(2012) 11 final (25/1/12), Article 17 (2).
[256] Ibid.
[257] *GDPR*, Article 17.
[258] As recently as 2017, the UK Government has called for opinions regarding the new Regulation's rights and derogations, in particular its freedom of expression exception within Article 85. It asked for submissions addressing how the Regulation could be implemented in a way which minimises disruption to business activities. See 'Government "Call for Views" on GDPR Derogations' (*Inforrm*, 19 April 2017) accessible at: https://inforrm.wordpress.com/2017/04/19/government-consultation-on/ (last accessed 28/4/17).
[259] In particular, image–based posts with a humorous element have a higher chance of being shared widely and becoming viral: See Noah Kagan, 'Why content goes viral: what analyzing 100 million articles taught us'

actions individually against every subsequent host website. Sartor has criticised Article 17(2) as 'burdensome' for controllers,[260] however, large websites such as Google or Twitter may often find it relatively easy to contact third party controllers when contrasted with a private individual, due to their available funds and stored information regarding web–usage.[261]

D. Domestic Purposes Exemption

Similarly to the 1995 Directive, the GDPR contains a so-called 'domestic purposes' exemption. Article 2(2)(c) GDPR states that 'this Regulation does not apply to the processing of personal data…by a natural person in the course of a purely personal or household activity'; recital 18 also details that the GDPR does not apply to:

> '…the processing of personal data by a **natural person** in the course of a **purely personal or household activity** and thus with no **connection to a professional or commercial activity**. Personal or household activities could include correspondence and the holding of addresses, or **social networking** and online activity undertaken within the context of such activities. However, this Regulation applies to **controllers or processors which provide the means** for processing personal data for such personal or household activities.'[262]

Questions have therefore been raised as to whether a third party can be held to account by the GDPR when posting personal data concerning another online – as the above excerpt of Recital 18 notes that personal processing in the context of social networking could be classed as a domestic purpose and exempt. Erdos has found that Data Protection Authorities, when seeking to navigate the domestic services exemption under the 1995 Directive, often drew a distinction regarding whether data was published to a large group – the larger the group, the

(*OkDork*, 21 April 2017) accessible at: http://okdork.com/why-content-goes-viral-what-analyzing-100-millions-articles-taught-us/ (last accessed 28/4/2017).

[260] Giovanni Sartor, 'The Right to be Forgotten in the Draft Data Protection Regulation' (2015) 5(1) *International Data Privacy Law* 64, 69.

[261] Forbes estimated that Twitter's 'fundamental value' was 15.7 billion – see 'In Any Acquisition, This is What We Think Twitter Is Worth' (*Forbes*, 26 September 2016) accessible at: https://www.forbes.com/sites/greatspeculations/2016/09/26/in-any-acquisition-heres-how-much-we-think-twitter-is-worth/#559440f2649a (last accessed 28/4/17).

[262] *GDPR* [emphasis added].

less likely that this publication would fall under the domestic purposes exemption.[263] Erdos says of the difference in approaches of national Data Protection Authorities ('DPAs'):

> 'EEA [European Economic Area] DPAs have generally adopted a strict approach to the application of data protection law to individual publication, **although considerable variation between the different regulators is also evident...**
>
> The vast majority (although not all) DPAs hold that once personal information relating to somebody other than the publisher themselves is disseminated to an **indefinite number**, the personal exemption cannot apply…'[264]

This approach is consistent with the case of *Lindqvist*[265] in which the CJEU held that a woman posting the personal data of her colleagues on her own personal website did not come under the scope of 'household activity' because of the large potential audience online that the data was exposed to.[266] Using this approach, a key issue in the '*third party poster*' scenario would be how visible a social media or other webpage was; Facebook and other social media sites allow an individual to restrict access to the information posted.[267] If *Lindqvist* is followed in this regard by the CJEU and other European (and the English) courts in interpreting the domestic purposes exemption under the GDPR, a crucial consideration would be whether a webpage was 'public' or private – and if the webpage was 'semi-restricted' (in other words, only certain people had access to it) how wide this group was; the wider the group, the less likely that the domestic purposes exemption could apply.

In general, Erdos has also noted that the UK and Irish Data Protection Authorities have adopted a much more permissive stance to the above, which 'appear[s] to ignore the responsibility of individual publishers here entirely'.[268] This is problematic for data subjects seeking redress in the '*third party poster*' scenario – where a data subject attempts to use their rights against the poster themselves. However, it must be noted that it would be more logical for a data subject to seek redress not against the third party poster, but if possible, a

[263] *Brimblecombe and Phillipson* and Erdos above, n 208 at 275. Erdos notes that a particular issue is whether the publication relates to an 'indefinite' number of individuals.
[264] Ibid Erdos, 276 [emphasis added].
[265] Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971.
[266] Ibid [47] and Erdos above, n 208.
[267] By making a page 'private' – Facebook operates a mechanism whereby one can vet who accesses their page by 'accepting' friends.
[268] Erdos above, n 208 at 276 and see *Brimblecombe and Phillipson*, 27-30.

corporation who is responsible for hosting the information – if they are also deemed a controller. As has been stated above, posters, administrators and website hosts including the likes of Facebook might be deemed jointly and severally liable as data controllers. Corporations such as Facebook will have more resources at their disposal to address any complaint raised under the GDPR, and a greater incentive to co-operate with a data subject. This incentive is both financial (due to fines imposed by the GDPR) as well as concerned with customer goodwill (a wish to preserve a public image as a company which values data protection).

How broadly this exemption will operate under the GDPR depends on how it is interpreted by national Data Protection Authorities and Member State courts (with possible guidance from the CJEU). This thesis would urge the UK and Irish Data Protection Authorities going forward not to minimise the responsibilities of individual publishers – if these are ignored, the deterrent effect of the GDPR against those breaching online privacy rights will be lost as will some of its ability to deliver an effective scheme across the UK and Europe. Individual posters who initially release private information into the public sphere are ultimately as culpable for breaching privacy rights as large websites which host this information – as but for the actions of this individual poster, the information may well have remained private. Indeed, the 2014 case of *František Ryneš* has been instructive regarding the domestic purposes exemption, Ausloos observing:

> ‘the CJEU [in the case] emphasised the exemption needs to be interpreted narrowly because:
>
> (a) the primary objective of data protection law is to ensure a ‘high level of protection of the fundamental rights and freedoms of natural persons’
>
> (b) ‘derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary’; and
>
> (c) the provision’s explicit reference to ‘purely personal or household activities’.

In sum, currently the household exemption needs to be interpreted *narrowly…*'[269]

Guidance from Article 29 Working party has followed suit behind *Lindqvist* and suggested that a 'informed decision' of a poster to disseminate personal data to the masses would render the domestic purposes exemption inapplicable in a given scenario.[270] Presumably, this means that if a poster realised they were posting another's personal data into the public domain and went ahead with posting this regardless, they could not be covered by the domestic purposes exemption – as they essentially have taken on the role of a data controller.[271] However, the guidance issued by Article 29 Working party has been inconsistent with regards to the *level* of emphasis it places on 'mass access' with regards to the application of the exemption. Despite the above position as stated by the Working Party in 2009, in 2013 it stated that this element to a case would *not be* pivotal – rather, it would merely be 'an important consideration'.[272] As Brimblecombe and Phillipson have noted, Article 29 Working Party's opinion with regards to the importance of mass disclosure and the domestic purposes exemption has undergone subtle changes in position as the years have progressed – they note by 2015 the Working Party restated that, despite pleas to the contrary (on the part of The Council of the European Union), the domestic purposes exemption must be interpreted 'restrictively'.[273] Regardless, what can be gleaned is that both the CJEU and Article 29 Working Party hold 'mass access' as one of the most important factors (and possibly *the most important* factor) in deciding whether the domestic purposes exemption applies.

What role, then, do any other factors play? Erdos has also suggested that more factors ought to play a part in the interpretation of this provision as opposed to just audience size – he has put forward several factors which he believes would give such a post severity and should therefore make it *less likely* that the exemption should apply.[274] These factors establish

[269] Ausloos and *Ryneš* above, n 227 at 150.
[270] *Brimblecombe and Phillipson*, 29 and Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, (2009) 01189/09/EN (WP163) at 6.
[271] Ibid.
[272] Article 29 Data Protection Working Party, Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package, (2013) Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities at 9 and *Brimblecombe and Phillipson*, 30.
[273] Article 29 Data Protection Working Party, Appendix: Core Topics in View of the Trilogue, (2015) Annex to the letters at 3 and *Brimblecombe and Phillipson*, 29.
[274] Erdos above, n 208 at 292 and *Brimblecombe and Phillipson.*

whether there has been a genuine breach of an individual's privacy.[275] Erdos' factors centre around the breach of privacy that has occurred – how serious it is, if it is 'offensive'[276] and include: 'its pejorative nature', 'disclosure of private details' (most particularly intimate ones such as data about one's sex life) and 'incessant and focused observation which amounts to a potentially unwarranted form of surveillance'.[277]

In interpreting the extent of this provision, a matrix of privacy 'balancing factors' could be relied upon by both national courts and Data Protection Authorities – detailed analysis and comments on some of these factors are laid out in the second part to this chapter (in relation to ECtHR caselaw). It is not difficult to envisage many additional factors being relied upon by a court in establishing whether the provision should apply; for example, a relevant consideration could be the effect the privacy breach has had on the claimant,[278] whether children are involved or impacted by the privacy breach[279] and perhaps even the motives of the third party who has posted the data to the internet. The precise development of this exemption under the GDPR remains to be seen – but given the CJEU's stance in *Lindqvist* and *Ryneš*, one can be cautiously optimistic that guidance from Europe will suggest a narrow approach to what qualifies as 'domestic purposes'. The UK's Information Commissioner gives two examples of domestic purposes as 'writing to friends and family…[and] taking pictures for your own enjoyment'[280] which interestingly makes no reference to personal data as made public. Indeed, data used within the home purely privately in this way is not the foremost concern of this thesis – as it is only when private information is made public with the potential for many to access it that informational privacy rights are significantly compromised online.

Therefore, to summarise:

I. The precise scope of the domestic purposes exemption under the GDPR remains unclear. Both the CJEU in *František Ryneš* and Article 29 Working Party (in some

[275] Article 8 privacy 'balancing factors' and the ECtHR will be discussed in the next section (part 2) of this chapter.
[276] Erdos above, n 208, 292.
[277] Erdos above, n 208, 292 and *Brimblecombe and Phillipson*, 20.
[278] C/f the 'serious harm' requirement under section 1 of the Defamation Act 2013.
[279] See *Weller v Associated Newspapers Limited* [2014] EWHC 1163 (QB).
[280] 'Exemptions', (*Information Commissioner's Office*), accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/?q=article+4 (last accessed 15/3/19).

instances) have, however, suggested a narrow approach to the exemption which prioritises data subjects and their privacy.

II. When seeking to determine the scope of the exemption, *Lindqvist* as well as the guidance of Article 29 Working Party shows that the potential audience size of that information is a key concern – if the potential audience is the 'whole internet' (information is unrestricted) the exemption will likely not apply.[281]

III. Aside from 'potential audience size' as a factor, Erdos has suggested that other factors may become relevant if a court seeks to determine the exemption's scope. Erdos' additional factors include: the sensitivity or intimacy of the information concerned (the more sensitive – the less likely the domestic purposes exemption will apply), whether the content is 'pejorative' (the content is personal and harsh, expressing contempt)[282] and the repeated nature of disclosures which harass a data subject. [283]

E. Consent to data processing in the GDPR

After the adoption of the 1995 Directive and the Data Protection Act 1998, multiple questions arose from legal practitioners, academics and business owners regarding the requirement of 'consent' to data processing. While the Directive requires that consent to processing be a 'freely given specific and informed indication' and Articles 7 and 8 of the Directive impose a requirement of unambiguous consent,[284] the Data Protection Act 1998 did not define consent.[285] This created a flurry of alarm in the UK with regards to whether consent was an 'active' or 'passive' exercise; in other words, whether the implied consent of a data subject to processing could ever be assumed by data controllers/processors or whether explicit consent

[281] *Brimblecombe and Phillipson*, 29.
[282] Ibid 30.
[283] Erdos above, n 208 at 292.
[284] *1995 Directive*, Article 2(h), Article 7a and Article 8 respectively.
[285] See the guidelines issued by the Information Commissioner's Office, 'The conditions for processing', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/ (last accessed 19/4/17).

was always required. In particular, organisations which processed personal data in relation to medical treatment raised concerns.[286] This lack of clarity in the Data Protection Act 1998 struck a stark contrast to the Directive's implementation in other EU Member States, all of which required continual assurances of consent to processing to be gathered on a rolling basis from data subjects.[287] According to Borghi, Ferretti and Karapapa in a 2011 survey, the majority of EU citizens preferred to specifically give their consent to data processing (rather than having their consent assumed).[288] Perhaps in part due to this confusion and inconsistency in approach,[289] the European Commission under the new Data Protection framework sought to enact a more robust and explicit consent mechanism in order to maximise privacy protection for data subjects. Within early drafts, the GDPR contained a 'clear and more straightforward' consent procedure, requiring data controllers and processors to obtain *explicit* consent to processing from subjects. Furthermore, a requirement was introduced for a subject to understand what they were consenting to, consent could be withdrawn at any time and an emphasis was placed on combatting the disproportionate bargaining power between large processing companies and private individuals.[290]

Despite the fact that Article 7 of the agreed text of the GDPR does allow for the subsequent withdrawal of consent,[291] the Commission's proposals for a requirement for 'explicit' consent were dropped as the GDPR passed through the European Parliament and was subject to redrafts.[292] The definition of 'consent' in the Regulation as finally enacted reads:

> 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.'[293]

Despite the earlier-proposed more rigorous rules being dropped regarding 'explicit' consent, this final definition does make clear that consent must be 'clear' and 'unambiguous'.

[286] See Townend et al above, n 215.
[287] Maurizio Borghi, Federico Ferretti and Stavroula Karapapa, 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK' (2013) 21(2) *Journal of Law Information Technology* 109, 119.
[288] Ibid, 111.
[289] As well as a rise in data processing during the 'digital age'.
[290] De Hert and Papakonstantinou above, n 204 at 136 as well as Costa and Poullet above, n 203 at 257.
[291] *GDPR*, Article 7 (3).
[292] De Hert and Papakonstantinou above, n 204 at 187.
[293] *GDPR*, (32).

Encouragingly, the phrasing of this definition seems to emphasise that a data subject's choices regarding their personal data and how it is processed should take priority as consent should not be assumed; rather, a subject must show their consent through an 'affirmative act'. By way of an explanation for this change, De Hert and Papakonstantinou have noted that due to advancements in technology, to require explicit consent from a data subject over every processing matter would be an impossible task.[294] It is easy to see how lobbyists at Member State as well as European Parliamentary level could (and did) make strong arguments against the inclusion of such a clause, as the requirement would take time and effort for a processor to implement. Consent forms would have to be carefully drafted and completed at various stages of data processing, costing processing businesses time, effort and money. The requirement of repeated and explicit consent would have provided an 'alert' procedure whereby a data subject would become aware of the extent of their personal data being processed as well as giving subjects a chance to reconsider their consent to processing afresh when a new consent form was required. If any consolation can be taken from this (partial) defeat on the part of data-rights, it is that Article 17 has transformed a removal of consent to processing (under Article 17(1)(b)) into an erasure request for private information.

The previous section of this chapter has discussed the new roles for national Data Protection Authorities, key definitions, the domestic purposes exemption and the role of consent in the GDPR. This chapter will now move its focus onto the rights that the Regulation confers on individuals over their personal data, which are central to the EU's new data protection framework.

F. Special category data

In its drafting, the GDPR differentiates between different types of personal data: that which is sensitive personal data, otherwise known as 'special category data' and that which is not. In its introduction, the Regulation states that 'sensitive personal data' by way of definition is:

> 'Personal data which are, by their nature, particularly sensitive in relation to

[294] De Hert and Papakonstantinou above, n 204.

> fundamental rights and freedoms…'[295]
>
> '[which] *merit specific protection* as the context of their processing could create significant risks to the fundamental rights and freedoms…'[296]

The GDPR goes on to say that:

> '…such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the *public interest* or in the exercise of official authority vested in the controller.'[297]

At first glance, then, the Regulation seems to require that particularly 'sensitive' types of personal data should not be processed *at all*, unless there is an extenuating circumstance in the form of certain specific cases, public interest, official authority or 'explicit consent' on the part of the data subject.[298] These provisions are fleshed out in Article 9 with an expanded list of what can constitute sensitive personal data (otherwise known as 'special categories of personal data'):

> '…personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation...'[299]

Article 9(2) also sets out the exemptions to this section, providing a list of *legitimate grounds* for processing special category data. This list can be summarised as:

(a) Explicit consent from a data subject for a specified purpose;

(b) [Processing is] necessary for a data subject or controller for exercising social security rights;

[295] *GDPR*, (51) [emphasis added].
[296] *GDPR*, (51).
[297] *GDPR*, (51).
[298] *GDPR*, (51).
[299] *GDPR*, Article 9(1).

(c) Necessary to protect the 'vital interests' of a data subject or of another natural person;

(d) Necessary for legitimate activities regarding politics, philosophy or trade unions;

(e) Processing relates to personal data which have *manifestly been made public by the data subject*;

(f) Processing relating to legal claims;

(g) Necessary for something in the substantive public interest;

(h) Processing in the interests of medicine…

(i) …public health

(j) …research.[300]

The last four exemptions on this list, (f)-(j) are similar to provisions in Article 17(3)(a)-(e), which also account for freedom of expression, compliance with legal obligations, processing relating to health, other types of research and legal claims.[301] At first glance, the amount of personal information that could be classed as *special category information* appears large – it ranges from a person's physical appearance to their religious beliefs. It also includes data that could be easily thought to be innocuous; philosophical opinions, for example – a discussion about which is not necessarily out of place between mere acquaintances. It is submitted that despite this broad 'catch-all' definition of special category data, the amount of information Article 9 will practicably be applied to is smaller than it initially appears. Although the list of what could be classed as special category data is long, the list of exemptions within 9(2) is longer. Article 9's exemptions also incorporate a degree of vagueness, as they fail to define what 'substantive public interest' would include and contain an exemption on the grounds of the 'vital interests' of a data subject or another.[302] However, the notion of 'explicit consent' to data processing has been kept within Article 9 whereas it was dropped from other parts of the Regulation with the fear of burdening website hosts and other types of social media operators.[303] This is interesting as it does demonstrate a desire from those drafting the Regulation that special category data should receive particularly robust protection, as the

[300] *GDPR*, Article 9(2). This list has been paraphrased for brevity.
[301] *GDPR*, Article 17(3).
[302] *GDPR*, where a data subject is unable to give consent.
[303] See above.

requirement of explicit consent implies the inclusion of a higher degree of written or oral confirmation, rather than the assumption that a data subject wishes their information to be processed.

For a controller to lawfully process special category personal data, they need a 'lawful basis' under Article 6 of the GDPR (a similar list to that above contained in Article 9, also including consent, necessity for a legal obligation and performance of a task in the public interest)[304] and to identify one of the above listed criteria – these two 'reasons' do not have to be the same or related.[305] This distinction between different types of data is similar to that made in Article 8 of the 1995 Directive and Data Protection Act 1998.[306] Like the GDPR, the 1998 Act also required data controllers to identify a particular ground for processing.[307] The idea behind these provisions appears to be that processing certain types of personal information poses more of a threat to an individual's rights than others – and in particular the types of information specified in Article 9 could be used to discriminate against a data subject.[308] However, if individual rights are to be protected comprehensively online this list of 'types of sensitive data' is problematic; it is both too wide and too narrow. As stated elsewhere in this thesis,[309] a person's political opinions can cover a broad array of matters, from what political party they support to what a person may think of same-sex marriage. The list also includes information relating to a person's sex life, but it does not elaborate; would this cover solely information as to who a person is having sex with, or does it also include sexual preferences and/or someone's sexual history? The answer to this may be no, as practitioners have noted that the original basis of this list of special category data was information that could be used to discriminate and the Equality Act 2010.[310] Therefore, someone's sexual orientation may be viewed as the most strongly protected type of information data in relation to special category data and sex-life. It is also difficult to ascertain whether Article 9's list is context-sensitive,

[304] *GDPR*, Article 6 (1)(a)(c) and (e).
[305] 'Special Category Data', (*The Information Commissioner's Office*), accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).
[306] *1995 Directive*, Article 8. The information was termed 'sensitive personal data'.
[307] 'Special Category Data', (*The Information Commissioner's Office*), accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).
[308] Ibid.
[309] See Chapter 5.
[310] Victoria Hordern, 'How do you solve a problem like special categories of data?'(*Data Protection Leader*, March 2018) accessible at: https://www.bwbllp.com/file/dpl-march-18-victoria-hordern-article-pdf (accessed 13/2/19) 8.

although the GDPR does not explicitly incorporate a test based on harm regarding the processing of special category data.[311]

The 2018 English case of *NT1 and NT2* concerned the disclosure of sensitive personal data.[312] Although the case was decided according to the 1995 Directive and the Data Protection Act 1998, some of its analysis remains relevant as there are many similarities between 'sensitive personal data' under the 1998 Act and 'special category' data under the 2018 Act and the GDPR, as discussed above. The two claimants in the case sought to order the delisting of links to reports of their criminal histories, which were protected as sensitive data under 2(g) of the 1998 Act.[313] Due to this, Google attempted to rely on a number of provisions within schedule 3 of the Act as *legitimate grounds* for the processing of such data.[314] Lord Justice Warby concluded that Google could successfully rely on schedule 3(5) – a ground which renders processing legitimate if *the data subject has made the personal data public themselves*.[315] He noted that if a person commits a criminal offence, they are in effect publicising their own personal data concerning their conviction – as they should have known that criminal offences are a matter of public record, and no other 'deliberate step' is required.[316] This reasoning is problematic - it persists despite the fact a claimant hasn't engaged any positive activity to make an offence or conviction public apart from the initial act of committing it (a matter unlikely to be at the forefront of an offender's mind while perpetrating a crime).[317] As Hugh Tomlinson QC, counsel for the claimants in the case, argued:

> 'the Claimant took no steps, deliberate or otherwise, to "make the information contained in the data" public. Condition 5, he says "requires some act of dealing with information". An offender such as NT1, who commits an offence in private, is by no

[311] Ibid.
[312] *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB) [53] (hereafter 'NT1 and NT2').
[313] Data Protection Act 1998.
[314] Data Protection Act 1998, Schedule 3. Some of these legitimate reasons include: consent on the part of a data subject, the administration of justice and the legitimate rights of another.
[315] Data Protection Act 1998.
[316] *NT1 and NT2* [111]. Lord Justice Warby here seeks to rely on the judgment of *Townsend v Google Inc* [2017] NIQB 81.
[317] See Alastair Sloan, 'NT1 and NT2: forgetting past misdemeanors' (*Information Law Blog*, 14 April 2018) accessible at: http://infolawblog.com/tag/journalism-exemption/ (last accessed 27/3/19).

means deliberately making his conduct public.'[318]

In terms of this thesis, this reasoning of Tomlinson's could also be applied to a situation where a data subject discloses personal data to a restricted group online, for it then to be spread more widely without their consent – the '*restricted access*' data-leak scenario. In addition, Sloan has noted that this argument made by the court is unsound as it hinges upon the premise that Article 8 of the 1995 Directive is unclear – a premise, which he and Tomlinson argue, is incorrect.[319] Article 8(e) simply states that a ground for legitimate processing of sensitive data is if 'the processing relates to data which are manifestly made public by the data subject'.[320] It could be argued that the term 'manifestly' actually goes some way further to imply that a deliberate, conscious act has been taken by a data subject in order to publicly distribute the data.[321]

As argued in Chapter 2, a certain piece of information disclosed or processed may seem trivial to one data subject, but not to another – depending on different lifestyles and a person's relationships.[322] There may also be problems with Article 9 which go beyond the scope of its data-list. Žliobaitė and Custers have argued that to combat discrimination, *increased* amounts of personal data-processing may actually help; for example, systems put in place to *recognise* that a job candidate was from a minority group and ensure that they are not discriminated as a result.[323] How effective Article 9 of the GDPR will be at protecting genuinely sensitive types of personal data remains to be seen. This will depend on how these requirements are interpreted in the national courts, including how generously the above listed 'processing grounds' are found to be. If the answer is very generously, Article 9 may have little effect at all. Its impact will also depend on how broadly these categories of data are drawn; the more information they are found to encompass, the more information will be given elevated protection.

[318] *NT1 and NT2* [110].
[319] Sloan above, n 317.
[319] *NT1 and NT2,* [110].
[320] *1995* Directive, and see *NT1 and NT2,* [113].
[321] *NT1 and NT2* [113].
[322] See chapter 2.
[323] Indrė Žliobaitė and Bart Custers, 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models' (2016) 24 *Artif Intell Law* 183.

Under the GDPR, Member States are permitted or, in some cases, *required*, to introduce supplementary national legislation detailing the precise terms of derogations from the new data protection regime – this includes exempting journalists from these processing rules regarding special category data in accordance with the journalism exemption in Article 85 of the Regulation.[324] Accordingly, paragraph 26(9)(a)(v), Part 5, Schedule 2 of the UK's Data Protection Act 2018 exempts journalists from the application of Article 9 in alignment with Article 85 of the Regulation.[325] However, an additional safeguard for journalists is in place in Schedule 1 of the new Data Protection Act, which exempts them from the laws applying to special category data: the section employs a heightened test of 'substantial public interest' which is clearly intended to answer to the particular sensitivity of the personal information covered by Article 9.[326] Wallace has noted that this is a 'belt and braces' approach and that it is difficult to envisage why this additional safeguard would ever need to be relied upon in addition to the exemption in paragraph 26, Part 5, Schedule 2.[327] At the very least, it is comforting for privacy advocates that reliance on journalism's second exemption within Schedule 1 contains an increased threshold regarding special category data.

G. Data protection principles

Article 5 of the GDPR contains a list of 'Principles relating to the processing of personal data'.[328] All personal data in the EU must be processed according to these principles, which are similar to those in Article 6 of the 1995 Directive.[329] The Regulation's principles can be summarised as such:

Processing must be:

(a) lawful, fair and transparent;

(b) collected for a specific purpose and not to be processed contrary to that purpose;

[324] *GDPR.*
[325] *GDPR.*
[326] Greg Callus, 'GDPR and journalism: the new regime' (*Inforrm*, 5 June 2018) accessible at: https://inforrm.org/2018/06/05/gdpr-and-journalism-the-new-regime-greg-callus/ (last accessed 4/12/18) and the Data Protection Act 2018, Paragraph 13, Part 2 Schedule 1.
[327] Ibid.
[328] *GDPR.*
[329] *1995 Directive.*

(c) adequate, relevant and limited to the necessity of that purpose;

(d) accurate;

(e) data must only be kept in a way which identifies a data subject if necessary for the processing purpose;

(f) secure.[330]

Offering guidance to data controllers as to Article 5 compliance, the UK's Information Commissioner states that 'these principles should lie at the heart of your approach to processing personal data'.[331] The principles form a cornerstone for data protection rights contained within the Regulation. As a whole they seem to emphasise that data should only be processed if *necessary* and only in a way that is compliant with a given purpose, limiting the ability of data controllers to use personal data at their discretion once it has been disclosed to them. These principles are not individual rights in of themselves, but rather guidelines as to the way a controller should approach handling personal data: broadly stated, it should be handled in a way which minimises the amount of personal data processed.[332] Principle (f) in particular emphasises that personal data must be handled responsibly.[333]

Although these principles are closely aligned to those set out in the 1995 Regulation (in particular, principles (a)-(e)), there have been some modifications.[334] In contrast to the Directive, individual data subject-rights are set out in dedicated sections of the Regulation away from the principles, in a way that gives rights greater emphasis and expanded definitions.[335] The UK's Information Commissioner advises that in order to prove compliance with data protection principles, a controller must have 'appropriate processes and records in place'.[336] As the Commissioner warns, Article 85(a) within the GDPR details that

[330] This has been paraphrased for brevity from Article 5(a)-(f) of the *GDPR.*
[331] 'The principles', (*The Information Commissioner's Office*), accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).
[332] One of the principles, (c), has in fact been termed 'data minimisation'.
[333] Also see 'The principles', (*The Information Commissioner's Office*) accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).
[334] Ibid.
[335] Ibid.
[336] 'The principles', (*The Information Commissioner's Office*) accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).

failure to comply with Article 5 leaves controllers liable for the highest tier of administrative fines.[337] The impact of Article 5 is potentially broad, as there is evidence that the Regulation's principles will impact upon how data controllers interact with third parties. Advisory websites have suggested that controllers ensure compliance with the GDPR's principles by discussing and implementing a data protection scheme, which would also apply to any third parties who work for the controller.[338]

H. What is the 'right to be forgotten'?

Article 17 allows 'data subjects' to obtain from 'data controllers' (including website hosts, authors of a webpage and search engines)[339] deletion of personal data concerning themselves online. It also contains a requirement for controllers to contact third parties in relation to the replication or repetition of personal data that has been requested for deletion under Article 17(2). The right is broadly framed, with the above roles loosely defined[340] and does not require a 'threshold of seriousness' to be met relating to a data privacy breach in order to invoke the right.[341] Article 17 appears to apply both to information initially uploaded to the internet by a data subject themselves and personal information uploaded by a third party. A (potentially) significant limitation upon the right is in the form of Article 17(3)(a), stated above, which contains an exception relating to the exercise of freedom of expression in relation to the activities of the data controller,[342] as well as the GDPR's journalism exemption in the form of 'special purposes', which will be discussed later in this chapter.[343]

The GDPR has extraterritorial effect and applies to 'the processing of personal data of data subjects who are in the Union by a controller or processor **not** established in the Union, where the processing activities are related to…the offering of…services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union',[344] theoretically including a service such as providing a social network like Facebook (of which

[337] Ibid.
[338] 'General Data Protection Regulation (GDPR) – Data protection principles' (*Nibusinessinfo.com*) accessible at: https://www.nibusinessinfo.co.uk/content/data-protection-principles-under-gdpr (last accessed 28/11/18).
[339] See *Google Spain*, where the CJEU found that search engine Google could constitute a data controller and see *GDPR*, Article 4.
[340] *GDPR*, Article 4.
[341] As opposed to, for example, a defamation claim brought under the Defamation Act 2013 (see section 1).
[342] *GDPR*, Article 17(3)(a).
[343] *GDPR*, Article 85.
[344] *GDPR*, Article 3.

operation is primarily based in the US). The CJEU has also demonstrated its willingness to apply EU data protection laws to companies whose central domain is outside of the EU, providing that they have a subsidiary base within it (largely common practice for large search engines or social networking sites).[345]

I. Why did the right to be forgotten come about?

The GDPR and the right to be forgotten can be seen as the first step in the right direction for Europe in addressing the speech-privacy imbalance that (this thesis argues) currently prevails online, affording EU citizens the ability to regain a modicum of control over their personal data on the web. There was no right within the 1995 Directive which exactly resembled the right to be forgotten, however a data subject had a right to deletion, correction [or compensation] from a controller if personal data processed about them was inaccurate or sensitive and the controller had not complied with the data protection principles.[346] There is no requirement for personal information to be 'sensitive' in order to exercise the right to be forgotten.[347] When the inclusion of the right to be forgotten within the first draft of the GDPR was announced it generated a significant amount of publicity, along with an outcry that it would lead to 'censorship' online, was unworkable in practice and compromised freedom of expression.[348] Part of the reason that the right generated such attention was that the majority of EU citizens did not know that the 'old' data protection framework – the 1995 Directive – contained an erasure mechanism. It is on this issue that the controversial case of *Google Spain* turned in 2014. It is important to set the case in context; at the time, the new GDPR was in the process of being re-drafted but had not yet been formally adopted. Many academics both in Europe and further afield had been vigorously debating the merits of

[345] See *Google Spain*. In this case the CJEU applied rules contained within the Data Protection Regulation 1995 to the search engine Google (which central domain is within the US) based on the fact it operates a subsidiary company in Spain.
[346] *95 Directive*, Article 12, 'The right of access' and Article 14, 'The data subject's right to object'. Also see Sartor above, n 260 at 65.
[347] *GDPR*, Article 9. Article 9 automatically outlaws the processing of certain types of sensitive data, including: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation (this is just a sample).
[348] See for example Meg L Ambrose, 'It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten' (2013) 16(2) *Stanford Technology Law Review* 369, Jeffrey Rosen, 'The Right to be Forgotten' (2012) *Stanford Law Review Online* 88, Diane L Zimmerman, 'The "New" Privacy and the "Old": Is Applying the Tort Law of Privacy Like Putting High Button Shoes on the Internet?' (2012) 17 *Communications Law and Policy* 107, Paul Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 *Harvard Law Review* 1966 and W. Gregory Voss, 'One year and loads of data later, where are we? An update on the proposed European Union General Data Protection Regulation' (2013) 16(10) *Journal of Internet Law* 13.

Article 17 – often critically.

The claim arose as Spanish national Mr González had requested the deletion of a link from search engine Google to a web-page which detailed that he had accrued social security debts 16 years prior to the case.[349] The Court held that a deletion right was present within the 1995 Directive and used several different sections of the Directive to dictate its scope. Firstly, it used Article 12 of the Directive, which states that a data subject can obtain:

> '(b) as appropriate the **rectification, erasure or blocking** of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or *inaccurate nature* of the data;'[350]

Secondly, the court focused on Article 6, which stated that data as processed:

> '(c) [must be] *adequate, relevant* and *not excessive* in relation to the purposes for which they are collected and/or further processed;'[351]

In other words, the court drew on the Article 12 deletion right for data which is not processed in accordance with the provisions of the Directive – in particular, because it is inaccurate. The court also referenced Article 6's requirement that data processing must not be excessive to justify their order requiring delisting of the relevant links from Google Spain,[352] to the relief of Mr González, who had been embarrassed that the information was easily accessible online through the search engine. The court also referenced Article 14 of the Directive, which gives data subject a 'Right to Object' to data processing, similar to that contained in the GDPR.[353] Article 29 Working Party released guidance on the ruling, which contained a restatement of importance of individual rights trumping over the competing 'economic interest[s]' of search engines and rights of individuals to consume information from the

[349] *Google Spain* [98-99]. For comment on the ruling see Sylvia de Mars and Patrick O'Callaghan, 'Privacy and Search Engines: Forgetting or Contextualising?' 43(2) *Journal of Law and Society* 257, 259 onwards.
[350] *1995 Directive* [emphasis added].
[351] *1995 Directive* [emphasis added].
[352] *Google Spain* [92-93].
[353] *1995 Directive.*

internet.[354] The ruling of *Google Spain* did potentially have a broad scope, as the Working Party noted:

> 'The ruling is specifically addressed to generalist search engines, **but that does not mean that it cannot be applied to other intermediaries**. The rights may be exercised whenever the conditions established in the ruling are met.'[355]

This potentially wide scope of the ruling is undoubtedly one of the reasons that the decision was deemed controversial at the time.

II. Article 17 GDPR

Recital 65 of the GDPR notes that the Article 17 right is particularly 'relevant' regarding the removal of personal data uploaded when the subject was a child. It also notes that the right of freedom of expression will be the most significant exception to Article 17, justifying the retention of data.[356] Article 17 reads as follows:

> '1. The data subject shall have the right to **obtain from the controller the erasure of personal data** concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> (a) the personal data are **no longer necessary** in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject **withdraws consent** on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
>
> (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

[354] Article 29 Data Protection Working Party, Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12 (26 November 2014) accessible at: https://www.dataprotection.ro/servlet/ViewDocument?id=1080 (last accessed 28/7/19), 2.
[355] Ibid [17 – emphasis added].
[356] Chapter 4 of this thesis contains an assessment of freedom of expression caselaw in the ECHR and English courts, suggesting a particular interpretation of Article 17's freedom of expression exception (with a view to enhancing data privacy rights online). *GDPR.*

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising **the right of freedom of expression** and information…'[357]

Some doubt has been expressed by academics with regards to the scope of Article 17(1)(a): the right to delete when the processing of personal data is no longer 'necessary'. A simple reading would render the section effective when consent to processing expires (if a time limit has been set) or the initial purpose of processing has been rendered null or void due to the passage of time. Sartor has questioned whether this would encompass data processing *complementary* to the processing initially consented to.[358] It seems logical that this would be the case, as due to the complexity of modern processing operations, it is likely that personal data will be processed in a number of different manners in order to achieve a previously agreed purpose. Interpreting the section in this way would ensure that personal data that is processed in a 'fringe' capacity would also be removed under Article 17, ensuring a comprehensive erasure mechanism for data subjects. For example, when a person creates an account on a dating website (such as 'Plenty of Fish' or 'Okcupid'), in addition to uploading personal data to form a page about themselves, they are often asked questions about their preferences regarding physical appearance.[359] It is possible that this information (which is

[357] *GDPR* [emphasis added].
[358] Sartor above, n 260 at 65.
[359] See 'Okcupid' and 'Plenty of Fish', accessible at: http://www.cupid.com/ppc.php?dynamicpage=cp_wlp_5step_t&utm_source=ppc&utm_term=gbr&utm_medium=web&utm_account=cupid_gbr_web&utm_campaign=731084815&utm_group=41908851807&utm_keyword=kwd-929779475&keyword=okcupid and http://uk.pof.com/ (last accessed 12/4/17).

stored by the application's data controller and sometimes publicly displayed) would be considered data processed in a complementary manner – as the purpose of personal data processing initially consented to was to create a personal webpage on the site, rather than to gather additional personal data as to how the operation of the application could be tailored.

In relation to Article 17(1)(b), an erasure right could become engaged in a scenario where consent to processing has initially been given by data subject and subsequently revoked, with no time limit in operation.[360] A subject may withdraw consent to processing that they have previously given under Article 6(1)(a):'the data subject has given consent to the processing of his or her personal data for one or more specific purposes' or Article 9(2)(a), which is akin to Article 6(1)(a) but applies to 'special categories' of personal data.[361] It must be noted that revoking consent will only generate a deletion request under Article 17 where there is no other lawful ground for processing, which can in turn depend on whether data is deemed 'sensitive'. As Brimblecombe and Phillipson put it:

> '…withdrawal of consent grounds a claim *only* where the previous consent of the data subject was the sole lawful basis for processing the data. Thus for "ordinary data", the controller could rely instead on their "legitimate interests" (unless overridden by the privacy interests of the data subject) as a lawful basis for processing. If the data is "sensitive" within the meaning of Article 9, the controller could seek to rely on a deliberate decision by the data subject to make the data public in the past, such as posting it to a public website as the basis. If this condition was found to be made out, then withdrawal of consent *per se* would not appear to ground a deletion request.'[362]

Indeed, section 9(2)(a) states that a prohibition on the processing of special category data does not apply if 'the data subject has given explicit consent to the processing of those personal data for one or more specified purposes'[363] and 6(1)(a) states that data processing is lawful if 'the data subject has given consent to the processing of his or her personal data for

[360] As this would, it is submitted here, come under the remit of Article 17(1)(a). C/f. Sartor above, n 260 at 65.
[361] As stated earlier in this chapter, this includes 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' according to Article 9(1) *GDPR.*
[362] *Brimblecombe and Phillipson*, 26.
[363] *GDPR.*

one or more specific purposes'.[364] Sartor has aptly observed that under (1)(b) processing only becomes unlawful after a data subject has withdrawn their consent and notified a controller.[365] Another ground for deletion under Article 17(1)(c) is that a data subject objects to their personal data being processed – Article 17(1)(c) states:

> 'the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)'[366]

Article 21 states:

> '1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her…including profiling based on those provisions. The controller shall no longer process the personal data unless the **controller demonstrates compelling legitimate grounds for the processing**…[367]

Presumably, if a data subject objects to processing pursuant to Article 17(1)(c) and there are no 'compelling legitimate grounds for the processing' then the processing of this data would be required to cease and the information would be erased, or at least removed from public access. The right is, after all, contained within the GDPR's 'erasure' Article. What can be inferred is that data 'timelines' are crucial in the interpretation of Article 17.[368] A person's right to object to personal data processing may initially be a weak claim,[369] however their claim may become stronger as the relevance of the personal data decreases and therefore the expression and public interest value of the data (if any) wanes.[370] Article 17(1)(d) also gives an erasure right to subjects when their data has been unlawfully processed, which could potentially be utilised by data subjects who have had their personal data uploaded to the internet by a third party. This data processing would be thereby rendered unlawful as consent to processing has not been given by a data subject in the first instance.[371]

---

[364] *GDPR.*
[365] Sartor above, n 260 at 65.
[366] *GDPR.*
[367] *GDPR,* Article 21 [emphasis added].
[368] Sartor above, n 260 at 68.
[369]For example, the claim may initially be weak due to the fact that the personal data in question relates to a matter of strong public interest – potentially engaging the freedom of expression derogation to Article 17 (see Article 17(3)(a) and Article 85 of the Regulation).
[370] Sartor above, n 260 at 68.
[371] See *GDPR,* Article 6, 'Lawfulness of Processing'.

I. Sanctions

In the GDPR's first draft Article 79(5)(c) stipulated that half a million Euro fine could be imposed upon 'anyone' who fails to comply with Article 17, or 1% of annual turnover in the case of a company.[372] The same held true for a breach of Articles 12-22, which spun the majority of individual data processing rights present in the Regulation; this included for example breaching Article 9, which concerns special category data and Article 18, the right to object to data processing. However, fines increased in the final draft of the GDPR. Breaching the data protection principles in Article 5 or sensitive personal data rights in Article 9 as well as Article 17 now entails a fine of either 20 million Euros or 4% of turnover according Article 83(5)(a) and (b).[373] The final draft of the Regulation also notes that the decision to impose either a 20 million Euro fine or a fine based on 4% of the annual turnover of a company will hinge upon *whichever is higher*.[374] This is a significant amount of money even for a large data controller such as Facebook or Google and an inordinately large sum for a smaller corporation. Despite this fact, the severity of this sanction can be defended on several grounds. Firstly, the fines are to some extent context-dependent; as stated above, a controller who is a large company with deeper pockets will be expected to pay more than a comparatively smaller company with less annual earnings if the *4% of turnover* fine is applicable. This helps ensure that this punishment is proportionate, which is important – Facebook's quarterly revenue in the last three months of 2016 was 8,809 million dollars,[375] whereas social networking site Bebo (popularised in the mid-2000s) was *sold* at one million dollars several years ago.[376] It is also vital to remember that these sanctions will not affect all companies who operate on the web equally: only corporations who process large amounts of

[372] Proposal for a Regulation of the European Parliament and of the Council on the protection of personal data and of the free movement of such data (General Data Protection Regulation) [2012] COM(2012) 11 final (25/1/12)Article 79(5)(c).
[373] 'The principles', (*The Information Commissioner's Office*), accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).
[374] *GDPR*, Article 83(5).
[375] Facebook Investor Relations, 'Facebook Reports Fourth Quarter and Full Year 2016 Results' (*Facebook,* 1 February 2017) accessible at: https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx (last accessed 21/8/17).
[376] See Catherine Clifford, 'Bebo founder buys back his website for $1 million and shuts it down right after' (*Entrepreneur,* 7 August 2013) accessible at: https://www.entrepreneur.com/article/227739 (last accessed 21/8/17).

personal data in a complex way are likely to be significantly affected.[377] The bigger the company, the more personal data it may process, and the greater the cost of implementing these new rules.[378] However, the size of a company often correlates to a larger financial output, so whereas companies processing significantly more personal data than others will be detrimentally affected, they may also be correspondingly larger and more affluent. An additional fact to note is that the powers of national authorities go beyond that of just fines in ensuring compliance: the UK Information Commissioner's Office has other powers, including issuing a controller with warning, suspensions on data processing, restrictions on transfers to non-EU countries and data erasure and amendment.[379] This range of different sanctions will ensure proportionality, as to present a data controller with a 20 million Euro fine for non-compliance without attempting to rectify a matter through other means may be viewed as unduly punitive.

Whether the substantial fines in the GDPR can be defended or otherwise, their strictness will likely encourage data controllers to comply with the increased data protection rights afforded by the Regulation. Indeed, within Article 83's opening paragraph (concerning administrative fines), the Regulation notes that one of the aims of the fines is to be 'dissuasive', as is the case with most financial penalties.[380]The severity of these fines is congruent with the EU Commission's general approach to the new Regulation in their implied emphasis on the importance of the personality rights of data subjects. Unlike other parts of the Regulation, their lack of interpretational scope will likely ensure that there is effective cross-European compliance with the new regime.[381] This is undoubtedly a good thing in terms of personal privacy on the web.

J. Article 17(3) and Article 85: exceptions to the right to be forgotten

[377] Gheorghio Gabriela and Spatariu Elena Cerasela, 'The EU General Data Protection Regulation Implications for Romanian Small or Medium-sized enterprises' (2018) XVIII *"Ovidius" University Annals, Economic Sciences Series* 88, 88.
[378] Ibid, 89.
[379] 'Penalties', (*UK Information Commissioner's Office*), accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/ (last accessed 6/4/19).
[380] *GDPR*, Article 83(1).
[381] Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (22 January 2012) available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (last accessed 18/6/15).

Article 17(3) sets out several exceptions to the right to erasure:

'…Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for *exercising the right of freedom of expression* and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.'[382]

These exemptions mirror those present within Article 9 pertaining to special category data.[383] In terms of this thesis, the most pertinent out of the five is 3(a), where processing is necessary for exercising the right of freedom of expression. It is on these terms that in English law, MPI claims are often denied, press freedom taking priority in those cases over individual privacy rights.[384] Article 85(1) GDPR also begins by stating:

> 'Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information...'[385]

The way Article 85(1) interacts with Article 17(3)(a) allows for an erasure right to be overridden by the right to freedom of expression. As Brimblecombe and Phillipson put it:

> 'On the face of it, it appears therefore that freedom of expression could be invoked to refuse deletion as a particular remedy, even where the data being requested for

[382] *GDPR*, emphasis added.
[383] See 'Special Category Data' above.
[384] See chapter 5.
[385] *GDPR.*

> deletion is being processed unlawfully. This might arise, for example, where the data requested for deletion is "sensitive" and there is no legal basis for processing it.'[386]

Chapter 4 will discuss potential interpretations of Article 17(3)(a) in detail, drawing upon Strasbourg Article 10 jurisprudence. For present purposes it may simply be noted note that this derogation will likely be the biggest obstacle for individuals seeking to enforce their Article 17 rights.

Article 85 goes into more detail regarding data processing and the GDPR's journalism exemption which is a different and separate 'defence' than 'freedom of expression', above. It is unclear as yet how different both of these sections will operate and interact in practice – they may in fact have a similar chilling effect on privacy rights, but this remains to be seen. It provides:

> '1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information [as stated above], including processing for *journalistic purposes and the purposes of academic, artistic or literary expression.*
>
> 2. For processing carried out for *journalistic purposes or the purpose of academic artistic or literary expression*, Member States shall provide for exemptions or derogations from [Articles 2-7 and 9]…[387]

As Article 85(2) states, it has been left to Member States to draft national implementing legislation specifying the precise terms of the journalism exemption.[388] In the UK's Data Protection Act 2018, the broad-brush journalism exemption appears in Schedule 2, paragraph 26. The Act dictates:

> '*Journalistic, academic, artistic and literary purposes*
>
> 26(1)In this paragraph, "the special purposes" means one or more of the following—
>
> (a)the **purposes of journalism**;

[386] *Brimblecombe and Phillipson*, 27.
[387] *GDPR* [emphasis added].
[388] *GDPR*.

(b)academic purposes;

(c)artistic purposes;

(d)literary purposes.

(2)Sub-paragraph (3) applies to the processing of personal data carried out for the special purposes if—

(a)the processing is being carried out **with a view to the publication by a person of journalistic, academic, artistic or literary material**, and

(b)the controller reasonably believes that the publication of the material would be in the **public interest**.

(3)The listed **GDPR provisions do not apply** to the extent that the controller reasonably believes that the **application of those provisions would be incompatible with the special purposes.**

(4)In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.'[389]

This exemption covers personal data rights including Article 17. Practitioners have noted that this 'special purposes' exemption has in fact widened 'in scope and application' under the 2018 Act as opposed to its counterpart in the Data Protection Act 1998.[390] It should be noted that to rely on the journalism exemption under 1998 Act's provisions, a controller must have only processed personal data for journalistic purposes *alone* (with no additional reason, aside from this, for processing).[391] Under Schedule 2, paragraph 26 of the new Act, this is no

[389] Data Protection Act 2018, Schedule 2, Part 5, paragraph 26 [emphasis added].
[390] Nicola Cain and Rupert Carter-Coles, 'GDPR and the Data Protection Act 2018 – how do they impact publishers?' (*RPC*, 28 May 2018) accessible at: https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/ (last accessed 14/3/19).
[391] Data Protection Act 1998, section 32.

longer a requirement.[392] Aside from this, the new Act's journalism exemption is similar in text to that of its 1998 predecessor.[393] It requires that:

I. the personal data must be processed with the intention to publish the information as journalistic material;

II. a controller's reasonable belief that doing so is in the public interest and;

III. a controller's reasonable belief that applying the relevant GDPR principle would hinder this journalistic motive – a set of criteria it shares with its 1998 counterpart.[394]

In terms of this final criterion, guidance from the Information Commissioner's Office has stated that this means that a data controller must think it impossible to apply the relevant GDPR provision while acting in a journalistic way.[395] There is a *subjective-objective* test within the special purposes exemption, in the sense that a controller must *subjectively* believe that the information is in the public interest and *objectively* reasonably believe that the special purpose the data was processed for would be incompatible with the data protection principles.[396] As with other aspects of the GDPR and the Data Protection Act 2018, how significantly this exemption will negate the right to be forgotten will depend on how it is interpreted. Certain phrases within the Act's drafting are ambiguous; it is unclear at this point how broadly the 'public interest' will be construed under 26(2)(b). As has been demonstrated by MPI caselaw, the English courts have been known to adopt inconsistent approaches to this concept. It has been held in *Ferdinand v MGN* that the private life of a footballer and his extra-marital affair had legitimate public interest value, but in *PJS* the English courts also held that the sex-life of a celebrity married couple *did not* attract the same level of public interest.[397] Hugh Tomlinson QC has noted that in interpreting this aspect of the Act (with

[392] Cain and Carter-Coles above, n 390 and Data Protection Act 2018, Schedule 2, Paragraph 26(3).
[393] Data Protection Act 1998, section 32.
[394] Cain and Carter-Coles above, n 390 and Data Protection Act 2018, Schedule 2, Paragraph 26(1)-(3).
[395] See 'Data Protection and journalism: a guide for the media', (*UK Information Commissioner's Office*) accessible at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf (last accessed 14/3/19) and Hugh Tomlinson, The "journalism exemption" in the Data Protection Act: Part I, the Law' (*Inforrm*, 28 March 19) accessible at: https://inforrm.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc/ (last accessed 14/3/19).
[396] *NT1 and NT2* and Sloan above, n 317. The defence here, interestingly, bears some resemblance to the section 4 public interest defence within the Defamation Act 2013 – where a defendant's publication must be in the public interest, and he must reasonably believe that the publication was in the public interest. This defence and defamation will be discussed in more detail in chapter 6.
[397] See chapter 5 of this thesis for a greater discussion about misuse of private information caselaw and the public interest.

reference to its 1998 predecessor), it is likely that the English courts will look to MPI jurisprudence, and that:

> 'the provision contemplates "public interest" justification for processing of a similar type to that required to justify the publication of private or confidential information: a belief that the public will be interested in the story or that publication of stories of that type is necessary for the economic viability of the publisher will *not be enough*.'[398]

Similarly, the 2018 Act fails to clearly state whether citizen (non-professional) journalists will be covered by Schedule 2's exemption. Phillipson and Brimblecombe observed that the CJEU in *Google Spain* held that search engine Google could *not* rely on the journalism exemption present within the 1995 Directive.[399] Despite this finding, the CJEU still left open the possibility for website hosts to rely on the exemption in certain circumstances,[400] and a pivotal issue may be whether a website is seeking to transmit 'information' or 'ideas' to the public.[401] The CJEU in the case of *Satamedia* suggested that the notion of 'journalism' under the 1995 Directive should be construed with a broad reading and encompass the notion of the *transfer of ideas*.[402] Somewhat confusingly, Tomlinson has also noted that the English case of *Sugar* contended that 'journalism' should *only* encompass the discussion of 'current affairs'.[403] This opens up the possibility for certain types of content on social media sites to be protected by the journalistic exemption, although not *all* content distributed by non-professional journalists will likely be protected under this heading – as to do otherwise would whittle away at the genuine definition of what it is to be a journalist.[404] Phillipson and Brimblecombe note:

> '…courts and regulators will, over time, have to engage in the extremely difficult task of classifying certain content on Twitter and Facebook as posted for journalistic purposes (e.g. comments on politics and current affairs), and some as not (e.g. family pictures). If the *content* is classified as falling within the "journalistic purposes"

[398] Hugh Tomlinson, The "journalism exemption" in the Data Protection Act: Part I, the Law' (*Inforrm*, 28 March 19) accessible at: https://inforrm.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc/ (last accessed 14/3/19) [emphasis added].
[399] *Brimblecombe and Phillipson*, 34-35.
[400] Ibid, 35 and *Google Spain* [85].
[401] Ibid *Brimblecombe and Phillipson* and Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831 [61].
[402] Ibid *Satamedia* and Tomlinson above, n 398 and *Sugar v BBC* (and another) [2012] 1 W.L.R 439.
[403] Ibid.
[404] *Brimblecombe and Phillipson*, 35-6.

> exemption, there would seem no good reason to hold that the individual poster *can* claim the journalism exemption but that the host (Facebook, Twitter) could not.'[405]

The new Act also notes that in order to use the exemption, a data controller must adhere to a relevant privacy code.[406] An example of such a code would be that put forward by the Press Complaints Commission in 2011, which has been adopted by its successor, the Independent Press Standards Organisation. The code states, among other things:

> 'i) Everyone is entitled to respect for his or her private and family life, home, health and correspondence, including digital communications.
>
> ii) Editors will be expected to justify intrusions into any individual's private life without consent. Account will be taken of the complainant's own public disclosures of information…'[407]

Adherence to this code is also taken into consideration by the English courts in MPI actions, in accordance with section 12(4)(b) of the Human Rights Act 1998.[408] This inclusion in the exemption is reminiscent of the journalism exemption in the Data Protection Act 1998, which stated that in considering whether the exemption applies, the English courts should take into account if the journalistic body had adhered to a relevant privacy code.[409] Callus has observed that although this appears a minute change in wording, it will mean that data controllers will have to be increasingly careful about compliance: as under the old regime, if a media outlet ignored privacy codes but happened to act in accordance with them, they could still rely on the exemption – this is not the case under the new Act.[410] Now, media outlets must be aware of relevant privacy codes and follow them explicitly in order to rely on this exemption. This will serve to strengthen a data subject's position when seeking to invoke Article 17 against a data controller who fails to comply with privacy codes.[411] Alongside other changes, paragraph 26 Part 5 Schedule 2 also increases the role of the UK's Information

[405] Ibid, 37.
[406] Data Protection Act 2018, Schedule 2, Part 5, paragraph 26(5).
[407] See Editors' Code of Practice, Independent Press Standards Organisation, available at: https://www.ipso.co.uk/editors-code-of-practice/#Privacy (last accessed 15/10/18).
[408] See chapter 5.
[409] And this in turn aligns with the position taken by the courts with regards to misuse of private information actions. See chapter 5 of this thesis and Section 12(4)(b) of the Human Rights Act 1998. Also see Callus above, n 326.
[410] Ibid.
[411] See James Theaker, 'Data Protection Bill – The future of the journalism exemption' (*Inforrm*, 28 November 2017) accessible at: https://inforrm.org/2017/11/28/data-protection-bill-the-future-of-the-journalistic-exemption-james-theaker/ (last accessed 4/11/18).

Commissioner in supervising media outlets' compliance with privacy codes (allowing the Commissioner to draft further guidance) and puts a review system in place to ensure that data subjects receive redress for data protection concerns, out of court.[412]

One can look to the English courts' first right to be forgotten-style case of *NT1 and NT2* for some suggestion as to how the GDPR's journalism defence will be interpreted in future – as although the case was decided under the 1998 Act, there is a great degree of overlap between both Acts' journalism exemption. *NT1 and NT2* concerned two separate but conjoined claims from two businessmen who had both been incarcerated in the past.[413] Both men had spent convictions and had requested the deletion of various links to articles discussing their former criminality from Google in light of the judgment in *Google Spain*.[414] Google denied several deletion requests in both cases and sought to rely on section 32 of the Data Protection Act 1998, the special purposes or journalism 'defence'. Ultimately, Lord Justice Warby found that the exemption did not apply to Google, and even if it had, then section 32(1)(b) would not have been met – which is the *reasonable belief* on the part of a controller that publication is in the public interest.[415] The judge did, however, make some interesting comments concerning the general construction and breadth of the journalism exemption in data protection law. Lord Justice Warby accepted that the exemption has a 'broad' reach under EU law,[416] and held that 'The concept extends beyond the activities of media undertakings and encompasses other activities, the object of which is the disclosure to the public of information, opinions and ideas.'[417] At first glance, this appears like an extremely generous reading of the exemption, however Lord Justice Warby moved quickly to put constraints on the exemption's scope in his next sentence, noting that not 'every' role within distributing information and ideas could be viewed as journalism, as to do so would 'elide the concept of journalism.'[418] This annex to his earlier comments is important – it makes clear that not simply *anyone* who spreads information online can claim a journalistic defence against the operation of data protection law. Lord Justice Warby seems to be implying that there is a

[412] See Callus above, n 326.
[413] *NT1 and NT2* [5-7].
[414] *NT1 and NT2*
[415] See Sloan above, n 317.
[416] *NT1 and NT2* [98].
[417] *NT1 and NT2* [98].
[418] *NT1 and NT2* [98].

difference between *genuine* journalism and journalistic activity and people merely spreading data on the web – a position commended and encouraged in this doctorate.

Lord Justice Warby also placed some general limits on search engines attempting to rely on the journalism exemption. Counsel for Google argued that because the search engine had facilitated access to journalistic material, it could invoke the journalism defence in the Data Protection Act 1998. They relied on section 32(1)(a) of the Act: 'processing is undertaken with a view to the publication ***by any person*** of any journalistic, literary or artistic material'.[419] The judge said of this argument:

> 'This narrower argument can be characterised, without meaning to disparage it, as **parasitic**. It depends upon the character of the underlying publication, and can only be relied on where that publication is for purposes properly characterised as journalism, or for one of the other special purposes. **Much material that people want to have delisted will not be within those confines.**'[420]

This appears to greatly discourage search engines seeking reliance on the journalism exemption moving forward under the Data Protection Act 2018, as Lord Justice Warby implies here that it will likely not apply to the majority of erasure requests under the GDPR – as the content concerned may well not be deemed 'journalistic'. The judge cemented his views in this regard by stating that Google's promotion of journalistic content was merely 'accidental'[421] and that there was 'no evidence' that Google gave the public interest any consideration when listing its results.[422]

Conclusion

To conclude, Part 1 of this chapter has attempted to give an overview of salient points in the GDPR and how they may relate to an individual attempting to remove personal data from the internet in 2019. It has described the new enhanced role for national Data Protection Authorities, analysed certain definitions in the GDPR and how they pertain to Article 17, and introduced the newly formulated right to be forgotten. As stated in the introduction, now

[419] Data Protection Act 1998 and Sloan above, n 317.
[420] *NT1 and NT2* [99 – emphasis added].
[421] *NT1 and NT2* [100].
[422] *NT1 and NT2* [102].

Article 17 has been introduced, Part 2 of this chapter will now move on to apply Article 8 ECtHR jurisprudence to the right to be forgotten. This caselaw and the principles that arise from it will act as a normative framework through which the new right will be examined.

Chapter 3, Part 2: How will Article 17 GDPR be interpreted according to Article 8 ECHR?

As noted earlier in this chapter, Article 17 is a broadly framed right and offers little guidance as to its proper interpretation, and in particular, how the tension it creates with freedom of expression, should be resolved. This section will consider the jurisprudence of the European Court of Human Rights (hereafter 'ECtHR') arising from its adjudication of claims under Article 8's right to respect for private life that give rise to competing Article 10, free speech, arguments. It will apply these approaches to potential actions which could be brought under the right to be forgotten or erasure and its interpretation, an analysis that has not yet been attempted in the literature.

This section of the chapter will work systematically through each of the key principles that may be derived from the ECtHR's privacy jurisprudence, evaluating how each one is either applicable to the interpretation of the right to be forgotten, applicable but with modification or inapplicable. In relation to each principle's application to Article 17, various data dissemination scenarios will be discussed pertaining to the disclosure of private data. Each factor employed by the Strasbourg court may apply differently to a claim under Article 17 depending upon, for example, whether the data subject has initially uploaded the personal information online themselves (and subsequently wishes to rescind its publication) or whether a third party has uploaded personal data concerning another, without their consent.

The section will firstly discuss Strasbourg's 'reasonable expectation of privacy' threshold test and the multiple different ways it could be applied to the right to be forgotten. It will then move to consider individual principles or factors that the ECtHR employs when assessing whether a reasonable expectation of privacy exists and the subsequent strength of a privacy claim. The weightier an Article 8 claim is, the more likely it will prevail over counteracting Article 10 (free expression) interests. Such factors include whether the private information relates to something occurring in a physically public location, the content of the personal data, whether the data subject in question is a public figure or a celebrity, implied 'waiver' of privacy rights, how the private data has been collected and disseminated and the format in which the information is disclosed. In chapter 4 of this thesis, the principles giving weight to competing Article 10 claims will be evaluated.

A. How is ECtHR caselaw relevant to the interpretation of a EU Regulation?

There are several key reasons why Strasbourg jurisprudence is informative in relation to the interpretation of EU secondary legislation. Firstly, the EU is involved in negotiations concerning accession to the European Convention on Human Rights (hereafter 'ECHR'), a move dictated by the Lisbon Treaty.[423] A draft accession agreement was drawn up in 2011, containing a 'co-respondent' procedure whereby the Union may join a Member State as a co-defendant to proceedings before the ECtHR in respect of human rights violations [424] as well as an internal review mechanism for the CJEU to review Union law and assess compatibility with the Convention. Importantly, the draft agreement grants the ECtHR external powers of review to scrutinise decisions of the CJEU in ensuring decisions are ECHR-compliant.[425] The most significant aspect of the EU's pending accession to the ECHR is that when this is complete Strasbourg jurisprudence will become formally binding upon the Union.[426] Unfortunately, some setbacks have occurred in relation to accession negotiations, the CJEU ruling in December 2014 that the draft accession agreement is incompatible with EU law.[427] In light of this, academics such as Peers have noted that amendments will need to be made to the agreement to appease the EU's court.[428] However, it remains the case that negotiations are ongoing and full accession in the future may well take place.

Secondly, Strasbourg jurisprudence is relevant to the interpretation and application of Union laws due to inter-court comity between the CJEU and the ECtHR. Both courts regularly cite

[423] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing European Community [2007] OJ C306/1, Article 6(2).
[424] A recent form of the draft accession agreement, dated 10 June 2013, can be viewed at: http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/Meeting_reports/47_1(2013)008rev2_EN.pdf (last accessed 14/4/16), the co–respondent procedure contained within Article 3.
[425] See Noreen O'Meara, '"A More Secure Europe of Rights?" The European Court of Human Rights, the Court of Justice of the European Union and EU Accession to the ECHR' (2011) 12(10) *German Law Journal* 1813, 1814 and Christina Eckes, 'EU Accession to the ECHR: Between Autonomy and Adaption' (2013) 76(2) The *Modern Law Review* 254, 254.
[426] Ibid Eckes at 254 and 279 and Christina Eckes, 'One Step Closer: EU Accession to the ECHR', (*UK Constitutional Law Blog,* 2 May 2013) available at: https://ukconstitutionallaw.org/2013/05/02/christina-eckes-one-step-closer-eu-accession-to-the-echr/ (last accessed 14/4/16).
[427] See Georgi Gotev, Court of Justice rejects draft agreement of EU accession to ECHR' (*EurActiv Blog,* 14 January 2015) accessible at: http://www.euractiv.com/section/justice-home-affairs/news/court-of-justice-rejects-draft-agreement-of-eu-accession-to-echr/ (last accessed 14/4/16) and Tobias Lock, 'The future of the European Union's accession to the European Convention on Human Rights after Opinion 2/13: is it still possible and is it still desirable?' (2015) 11(2) *European Constitutional Law Review* 239.
[428] Steve Peers, The CJEU and the EU's accession to the ECHR: a clear and present danger to human rights protection' (*EU Law Analysis Blogspot*, 18 December 2014) accessible at: http://eulawanalysis.blogspot.co.uk/2014/12/the-cjeu-and-eus-accession-to-echr.html (last accessed 14/4/16).

the other's judgments and look to each other for guidance,[429] in many cases the CJEU taking the ECtHR's more experienced lead when adjudicating upon fundamental rights.[430] Both courts have also been known to engage in the tandem deliverance of judgments over similar issues.[431] Over the course of the last decade a strong working relationship between both courts has been fostered, with relations between the judiciary of both courts good and members meeting extra-judicially to discuss judgments.[432] De Vries observes that 'lines are becoming increasingly blurred' between rights protection afforded between the ECtHR and the CJEU.[433] This strong bond between both courts demonstrates the influence that Strasbourg caselaw may have over the interpretation of the Union's new data protection framework.

The final, and most significant, reason that Strasbourg jurisprudence is relevant to the reading of Article 17 is the parallel rights to privacy enshrined within the ECHR (present in Article 8) and the Charter of Fundamental Rights of the European Union (within Article 7).[434] The EU's Charter is 'complementary' to that of the ECHR.[435] Article 52(3) of the EU Charter states:

> '3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the **meaning and scope of those rights shall be the same as those laid down by the said Convention...**'[436]

In essence, when Charter and ECHR rights align, the EU's charter states that the *meaning and scope* of both are to be taken to be the same[437] – although, Article 52(3) goes on to state that this does not mean that additional protection for such rights cannot be conferred by the

[429] O'Meara above, n 425 at 1815.
[430] Tommaso Pavone, 'The Past and Future Relationship of the European Court of Justice and the European Court of Human Rights: A Functional Analysis' M.A Programme in Social Sciences, University of Chicago (28th May 2012) 1.
[431] O'Meara above, n 425 at 1819.
[432] Ibid at 1816.
[433] Sylvia de Vries, 'EU and ECHR: Conflict or Harmony? – Editorial' (2013) 9(1) *Utrecht Law Review* 78, 79.
[434] Charter of Fundamental Rights of the European Union, (18/2/2000) OJ C364/3, Article 7 and *ECHR*, Article 8.
[435] Pavone above, n 430 at 3.
[436] Charter of Fundamental Rights of the European Union, (18/2/2000) OJ C364/3 [emphasis added].
[437] See Wolfgang Weib, 'Human Rights in the EU: Rethinking the Role of the European Convention on Human Rights After Lisbon' (2011) 7(1) *European Constitutional Law Review* 64, 64-67.

EU Charter.[438] As privacy is such an overlapping right, Strasbourg jurisprudence is directly relevant to the CJEU and European courts' formulation of Article 17.

It must also be noted here that obligations are present on the English courts to interpret existing English law in line with human rights under the ECHR. Under section 2(1)(a) of the Human Rights Act 1998, an English court, when deciding on a matter which relates to a human right – such as privacy – must take into account relevant judgments of the Strasbourg Court. Moreover, as an English court is a public authority according to section 6(3)(a) of the Human Rights Act 1998, it must interpret legislation (such as the Data Protection Act 2018 and the GDPR, which is retained law) in a way which is compatible with convention rights, as per section 3(1) of the Act. These provisions under the 1998 Act bolster the relevance of Article 8 jurisprudence to the English courts' interpretation of the right to be forgotten.

B. Scope of this chapter

As stated above, the EU's Charter of Fundamental Rights has coterminous rights with the ECHR – Article 8 ECHR (privacy) and Article 10 (freedom of expression) correlate to Article 7 and Article 11, respectively, of the Charter.[439] The Charter has an additional right that the ECHR does not have – Article 8, the right to protection of personal data. The right is not fleshed out in the Charter, it simply stating:

> '1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the **right to have it rectified.**
>
> 3. Compliance with these rules shall be subject to control by an independent authority.'[440]

[438] Charter of Fundamental Rights of the European Union, (18/2/2000) OJ C364/3, Article 52(3).
[439] Ibid the Charter.
[440] Ibid the charter, Article 8 [emphasis added].

Article 8 of the charter does not expressly discuss the right to erase personal data, but does reference the right to 'rectification' of personal data – which is presumably correcting data which is wrong and publicly accessible online, which does not equate to the *general deletion right* of the right to be forgotten. It does not seem at this stage that Article 8 of the charter will have a significant impact on the finer details of how Article 17 is interpreted. As noted in chapter 1, the decision has been made in this thesis to focus on Articles 8 and 10 ECHR because of the coterminous relationship between the rights of the Charter and the ECHR and the breadth of case law that can be drawn upon from the Strasbourg court on the key issue of privacy and free expression 'balancing' which will be pivotal for courts when interpreting the scope of Article 17 (and competing expression interests). Furthermore, this PhD examines the issue of privacy online from the standpoint of an individual in England and Wales; the UK is currently in the turmoil of Brexit and is soon to depart the EU,[441] after which caselaw from the CJEU *may* only continue to have influence over the English and Welsh courts.[442] The same cannot be said of ECtHR caselaw, which will continue to have direct relevance in English and Welsh courts due to obligations imposed by the Human Rights Act 1998. It remains to be said that certain past decisions of the CJEU have been instructive in this area, namely *Lindqvist*, *Satamedia* and *Google Spain*, all of which were referenced in the previous section of this chapter.

C. A preliminary note on different data dissemination scenarios

It is important at this juncture to restate the various different circumstances leading to personal data about a data subject being disseminated online. As mentioned above, the manner in which the information came to be accessible may affect how the 'balancing principles' employed by Strasbourg Court in adjudicating Article 8 claims would apply to the right to erasure.

I. Information concerning a data subject ('A') is uploaded by a third party ('B') without A's consent – the *'third-party poster' scenario*

[441] This looking increasingly likely as 'Brexiteer' Boris Johnson won the Conservative Party leadership contest in July 2019, and is at the time of writing Prime Minister. Johnson has promised Brexit by 31st October 2019.
[442] Section 6(2) and 6(3) of the EU (Withdrawal) Act 2018.

Personal data distributed online in this manner embodies the most significant parallels to traditional Article 8 claims according to ECtHR caselaw. The vast majority of ECtHR privacy jurisprudence concerns the non-consensual publication of personal information relating to an individual by a third party, often the press. It was under these circumstances that photographs were published in a German magazine of Princess Caroline of Monaco in the seminal case of *Von Hannover v Germany*.[443] More recently the celebrity couple Lars Lillo-Stenberg and Andrine Sæther brought a claim under Article 8 in relation to photographs of their wedding taken covertly and published by Norwegian magazine 'Se og Hør.'[444] Therefore the Strasbourg Court's principles pertaining to the weight of the Article 8 claim (such as whether the information relates to a public location and the content of the information) can be directly 'read-across' and applied to a potential claim brought under Article 17 whereby person 'B' uploads personal data to the Internet concerning person 'A', without their approval.

II. Person B publishes or disseminates information that contains personal data of person A without their consent *alongside* information concerning person B – *the 'mixed claims' scenario*

A further issue to be discussed within the second part of this chapter is a circumstance where a third party (B) uploads a photograph onto a social networking site which contains an image of themselves as well as another data subject (A); A objecting to its accessibility online. To unilaterally order deletion of such a photograph under Article 17 gives rise to a conflict in autonomy of the freedom of expression of person B, and the right to privacy of person A. As Gomery observes, this is a complex issue of 'whose autonomy matters?'.[445] This clash of interests is difficult to reconcile, yet Strasbourg principles relating to the strength of Article 10 rights in response to Article 8 claims can (to an extent) be applied in order to shed light on which right should prevail within this scenario.

III. An individual has posted personal data to a social networking site and the individual retains control over the data – the *'retained control' scenario*

[443] *Von Hannover.*
[444] *Lillo-Stenberg and Sæther v. Norway* App no 13258/09 (ECHR, 16 January 2014). Hereafter '*Lillo-Stenberg'.*

[445] Geoffrey Gomery, 'Whose autonomy matters? Reconciling the competing claims of privacy and freedom of expression' (2007) 27(3) *Legal Studies* 404.

If a data subject uploads personal information to a social networking site and retains access and control to that personal data, the individual is at liberty to delete personal information from the site themselves. Therefore, the individual would not need to invoke the deletion right contained within Article 17 – rather, they could simply remove the 'post' in question. Furthermore, social networking site Facebook allows users the option to either 'deactivate' their account (whereby it is no longer visible to others but personal data remains stored on company servers, enabling a user to reactivate their account at any time) or to permanently delete their profile (personal data permanently is erased from the company's database, and profiles cannot be resurrected).[446]

IV. A data subject (A) has voluntarily made personal data available online concerning themselves and this data has been reposted to third party sites (controlled by 'C'); A wishes to delete the information – *this covers both the 'restricted access' and the 'personal public disclosure' scenarios*

This is perhaps the scenario furthest removed from traditional claims under Article 8 ECtHR jurisprudence. As will be discussed below, the Strasbourg Court firstly applies a 'reasonable expectation of privacy test' (hereafter 'REP' test) to such a claim, utilising a selection of balancing factors, and if a reasonable expectation is found the Court then proceeds to consider the weight of the claim and how it can be reconciled with competing freedom of expression interests, using the same set of factors (perhaps with a different amount of emphasis on individual principles).[447] It will be argued within this chapter that the classical formulation of the REP test in relation to this data dissemination scenario is out-dated and ought not to be a requirement for an individual to *per se* invoke a claim under Article 17.[448]

This chapter will now move on to consider in detail how the REP test is applied to privacy claims by the Strasbourg Court and its relationship to the right to be forgotten. It will then

[446] The introduction of a 'permanent' deletion of a Facebook account is a modern introduction to the company, likely in response to users' dissatisfaction with the ability to only 'deactivate' rather than remove their page. See Sophie Curtis, 'How to permanently delete your Facebook account' (*The Daily Telegraph Website*, 19 August 2015) available at: http://www.telegraph.co.uk/technology/facebook/11812145/How-to-permanently-delete-your-Facebook-account.html (last accessed 17/4/16).
[447] See H. Tomás Gómez-Arostegui, 'Defining "Private life" Under Article 8 of the European Convention on Human Rights by Referring to Reasonable Expectations of Privacy and Personal Choice' available at: http://www.duo.uio.no/publ/jus/2004/21399/HTGA_Thesis.pdf (last accessed 18/5/16) 10.
[448] Indeed, it is not a requirement according to Article 17.

evaluate how the principles the ECtHR employs in assessing the existence of a REP and the subsequent weight of a privacy claim are applicable to claims that could potentially be brought under the right to erasure and its interpretation. It will be demonstrated that some ECtHR balancing factors/principles are directly relevant to an evaluation of Article 17 rights, some principles are relevant yet require a modification of approach and some principles are incompatible.

D. Analysis of European Court of Human Rights Article 8 jurisprudence

As stated above, when adjudicating an Article 8 claim, the ECtHR firstly evaluates whether the subject in question has a 'reasonable expectation of privacy' pertaining to the disclosed information. In deciding whether a reasonable expectation of privacy will arise, the Court will consider a list of factors, discussed below. If a REP is not established, then the claim will automatically fail; if a REP is established, the Court, in order to weigh up the Article 8 claim against Article 10 considerations, will once again consider the abovementioned list of factors which may give weight to the privacy claim (in not necessarily the same depth or order as it did to establish an REP).[449]

I. What is the reasonable expectation of privacy test?

Judge Zupančič in *Von Hannover v Germany* stated that 'reasonableness is…an allusion to informed common sense.'[450] Gómez-Arostegui observes that the Strasbourg Court makes a clear attempt to acknowledge the existence and importance of a REP test in a plethora of cases, including *Halford v UK*, *PG & JH v the UK*, *Peck v UK*, *Perry v UK* and more recently *Von Hannover v Germany* (*Nos 1, 2 & 3*), *Sæther v. Norway* and *Couderc v France*.[451] An example of Strasbourg's traditional application of the REP test is present in *Halford*. It was held in the case that a police officer's Article 8 rights had been breached through Ms. Halford's employers monitoring her phone calls at work. Ms. Halford had been informed by her workplace that she could use certain phones to discuss private matters without fear of

[449] The court is not obliged to take every factor into account – some may be irrelevant to the case.
[450] Gómez-Arostegui above, n 447 and *Von Hannover* [64].
[451] *Halford v United Kingdom* App no 20605/92 (ECHR, 25 June 1997), *PG and JH v United Kingdom* App no 44787/98 (ECHR, 25 September 2001), *Peck v United Kingdom* App no 44647/98 (ECHR, 28 January 2003), *Perry v United Kingdom* App no. 63737/00 (ECHR, 17 July 2003), *Von Hannover, Von Hannover v Germany (No.2)* App nos 40660/08 and 60641/08 (ECHR, 7 February 2012) hereafter '*Von Hannover (No.2)'*, *Von Hannover v Germany (No.3)* App no 8772/10 (ECHR, 19 September 2013) hereafter '*Von Hannover (No.3)'*, *Lillo-Stenberg, Couderc and Hachette Filipacchi Associes v France*, App no. 40454/07 (ECHR, 12 June 2014) and Gómez-Arostegui above, n 447 at 10.

external intrusion to the line (in particular to discuss matters relating to a grievance she was pursuing against the police force), thus a reasonable expectation of privacy on Ms. Halford's part arose.[452] In other words, Ms. Halford could not have reasonably foreseen that her personal telephone calls would be intercepted, as she had been specifically advised to the contrary.

II. Application of the reasonable expectation of privacy test to various claims potentially brought under a right to be forgotten

It is important to note that discussion regarding Strasbourg's REP test and how it may be used with regards to the right to be forgotten is, at this early stage, somewhat speculative. There are multiple different possibilities of how the English courts may utilise the REP test in order to colour their interpretation of the right to erasure – although it must be noted that a court cannot interpret a law *contra legem*. Also, the potential remains for the ECtHR to directly rule on the scope of the right to be forgotten if a claim is brought in the Strasbourg court against the right as infringing Article 10, freedom of expression, interests.

III. Different ways the REP test could be utilised by the UK courts in interpreting the right to be forgotten:

i. The English and Welsh courts could face pressure to 'read down' (in other words, narrowly interpret) the scope of Article 17 GDPR by importing the REP test as a threshold requirement to establish that the right to be forgotten can be relied upon by a data subject. This would be an extremely restrictive interpretation of the right to erasure, and indeed an interpretation that media bodies may lobby courts towards. It would appear unlikely that this interpretation would be adopted by the CJEU (as it would drastically reduce the scope of the new right - this will be discussed in detail below), however it is possible that the Strasbourg Court could take on this interpretation of Article 17 if it is challenged in the ECtHR on the grounds of infringing Article 10.

[452] *Halford* above, n 451 [44 and 45], Gómez-Arostegui above, n 447 'at 11 and Alastair R Mowbray, *Cases and Materials on the European Convention on Human Rights* (Oxford University Press 2007) 557-561.

ii. The English and Welsh courts may treat the REP test as irrelevant regarding a 'threshold' test in order to rely on the right to be forgotten, but:

iii. The courts may use the factors employed to establish a REP (and later to balance Article 8 claims against Article 10 interests) in order to reconcile an erasure claim under Article 17 against the freedom of expression exception to the right present in Article 17(3) (a).[453]

iv. Alternatively, a compromise between the above two situations could be drawn and the English courts may utilise the REP test as a threshold requirement to invoke the right to be forgotten only in doubtful or borderline situations, where the data requested for deletion is particularly contentious in some way. Some examples of such complex situations include:

a. Article 17's application regarding social media usage and the domestic purposes exemption: does the domestic purposes exemption apply and negate Article 17?[454]

b. Using Article 17 to request the erasure of 'sensitive personal data', but it is the data subject themselves who has made it public.[455]

c. Who is a data controller?[456]

d. In Article 6(1)(f) of the GDPR a controller can argue that data is being lawfully processed 'for the purposes of legitimate interests pursued by the data controller or a third party'. A data subject may seek to contest this and ask for their data to be erased under Article 17.[457]

[453] *GDPR*, Article 17(3)(a).
[454] See the above section on the GDPR's domestic purposes exemption in Chapter 3 part 1 and *Brimblecombe and Phillipson*, 44.
[455] According to Article 9(1)(c) of the GDPR, this could be another ground for the legitimate processing of such data apart from consent to processing, ibid *Brimblecombe and Phillipson*.
[456] The scope of this could potentially be extended, as it has been in the past regarding search engines. See the above section on data controllers in Chapter 3, part I and ibid *Brimblecombe and Phillipson.*
[457] *GDPR* and ibid *Brimblecombe and Phillipson* 44-45.

e. In general, the balance between Article 17 privacy rights and freedom of expression will have to be carefully struck (particularly as Article 17(3)(a) contains an exemption on the grounds of freedom of expression). The ECtHR's balancing factors could help guide courts as how to strike this balance.[458]

E. The REP test and different data dissemination scenarios

I. Information concerning a data subject ('A') is uploaded by a third party ('B') without A's consent: the 'third-party poster' scenario

Where a claim is brought under Article 17 relating to personal data uploaded online by a third party without consent, principles applied by the Strasbourg court under the REP test can be read-across to this scenario in a direct way. As stated above, the dissemination of private data relating to another by third parties is the traditional scenario whereby an Article 8 claim is brought before the ECtHR.[459] Furthermore, the Strasbourg court appears to have taken the processing of personal data relating to an individual by an external actor as a significant consideration in determining whether a REP exists. In the case of *PG and JH v the United Kingdom*, an Article 8 claim was brought relating to the recording of a detainee's voice while in a police station. The man in question did not know that he was being recorded and he was one of several men who had bugs placed upon their person while incarcerated without their knowledge.[460] The ECtHR held that as the men reasonably believed that they could only be heard speaking by the people physically present at the time, a REP arose.[461] In its finding of a violation of Article 8, the Strasbourg court appeared to focus upon the fact that the police had processed personal data in relation to an individual and there was a permanent record of the private information obtained.[462] Similarly, in the case of *Perry v the United Kingdom*, the claimant was covertly filmed at a police station, and a CCTV camera had been moved by the police in order to record a clear image of the man in question. The claimant argued this had

[458] *GDPR* and ibid *Brimblecombe and Phillipson* 44-45.
[459] See for example *Von Hannover*.
[460] *PG and JH* above, n 451.
[461] Ibid [57–60].
[462] See Council of Europe/European Court of Human Rights, 'Information Note on the Court's case – law no. 34: P.G. and J.H. v. the United Kingdom - 44787/9 (September 2001) accessible for download at Hudoc webpage, last accessed (18/4/16).

been a breach of his Article 8 rights – in particular due to the fact he did not know that the camera was there and it had been angled specifically in order to capture footage with greater detail.[463] The ECtHR held that the suspect did indeed have a partial REP and his Article 8 rights had been violated. Strasbourg expounded that this was firstly because the use of the CCTV camera went beyond what the claimant could have reasonably foreseen and crucially the device had been used to record the claimant's image and private data relating to the claimant had been processed (as was the case in *PG and JH*, above).[464]

As Gómez-Arostegui observes, it is clear that the processing of personal information without consent forms part of the assessment of an REP by the Strasbourg court.[465] The expectation may be full or partial; in other words, more or less significant.[466] Furthermore, in the case of *Amann v Switzerland*, the ECtHR appeared willing to find a breach of Article 8 rights – and a REP therefore present - in relation to personal data merely *stored* by a third party against a subject's wishes. It should be emphasised that the storage of personal data is a significantly less serious breach of privacy than the dissemination and availability of personal data online, as would be the case with a claim under Article 17.[467] If European and English and Welsh courts take the ECtHR's lead in placing what appears to be an increased importance upon breaches of Article 8 through the processing of personal data then this may render Article 17's interpretation with a duly flexible and wide ambit. Such an interpretation of the REP test is to be welcomed – as stated in the previous chapter of this thesis, it is essential that the protection of robust privacy rights is ensured in order to combat the increased threats to data protection which the digital age has heralded.[468]

II. A data subject (A) has voluntarily made personal data available online concerning themselves and this data has been reposted to third party sites (controlled by 'C'); the data subject wishing to delete the information

There are two sub-categories to this data dissemination scenario.

[463] *Perry* above n 451.
[464] Ibid [40–43].
[465] Gómez-Arostegui above, n 447 at 15.
[466] The idea of a 'partial' expectation of privacy will be discussed in more detail later in this chapter, particularly with regards to *Peck v United Kingdom*.
[467] *Amann v Switzerland* App no 27798/95 (ECHR, 16 February 2000) [70].
[468] *Delete.*

i. A data subject has uploaded personal data online to a restricted webpage, the data subsequently leaked and posted to third party sites – the 'restricted access' scenario

In a circumstance whereby an individual uploads personal information to a website believing that it would only be viewed by a restricted audience (for example, only approved individuals on social networking sites - such as 'friends' on Facebook)[469] and the data is taken by a third party and posted to other sites, leading to wider readership, it may be possible to conceive that a data subject has a partial REP. This is due to the fact that the subject could not have reasonably foreseen that the information would be viewed by such a large audience.[470] Indeed, this situation draws significant parallels to the case of *Peck v United Kingdom* as well as the abovementioned cases of *PG and JH* and *Perry*. *Peck* concerned stills of a CCTV recording distributed by the local council of Mr Peck's suicide attempt on a public street. Mr Peck's face was not distorted and he was holding a knife.[471] The ECtHR held that Mr Peck had a REP in relation to the broadcast: the Court noted that although the general public on the street at the time would have been able to view his actions, Mr Peck could not have reasonably foreseen that stills of the footage or the video itself would have been published in newspapers or broadcast to an audience of thousands (the images were broadcast countrywide on the BBC).[472] Similarly, in *PG and JH* and *Perry* the Strasbourg Court found the existence of a REP due to the fact the claimants' data had been processed in more extensive a manner than they could have reasonably foreseen.[473]

ii. A data subject has uploaded personal data to an unrestricted and publicly accessible website – the 'personal public disclosure' scenario

The application of Strasbourg's REP test to a circumstance whereby a data subject voluntarily uploads personal data to a publicly accessible online domain (and subsequently wishes for the data to be removed) is more problematic. Under these circumstances it is

[469] Individuals that data subjects have approved to have access to restricted personal information displayed online.
[470] In the case of *Peck v United Kingdom* the ECtHR stated that Mr Peck, who had attempted to commit suicide on a public street, had a partial expectation of privacy as he could not have reasonably foreseen that the stills of the CCTV footage of the event would be broadcast on television and distributed to other police constabularies other than that of his local. This case will be discussed in more detail later in this chapter.
[471] *Peck* above, n 451 [62].
[472] *Peck* above, n 451 [62] and Gómez-Arostegui above, n 447 at 17.
[473] *PG and JH* and *Perry v United Kingdom* above, n 451.

difficult to see how a data subject could be deemed to have a REP, as it appears reasonable for the claimant to have foreseen that in uploading data to a public platform that a large and, critically, unknown amount of users may view the information. The role of the data subject differs in this scenario from the position of most claimants within Strasbourg's Article 8 jurisprudence, as the subject has initially chosen to make the personal data open to view by the public *themselves* rather than the press or another third party doing so through an independent exposé. They have voluntarily surrendered control over the data, and who accesses it.[474] The REP test focuses upon what degree of privacy breach a claimant could have reasonably foreseen occurring (*Peck, PG and JH* and *Perry*),[475] whereas Article 17 GDPR emphasises the importance of a data subject's ability to rescind their previous publication of private data when a subject subsequently 'withdraws consent' to processing.[476] Article 17 prioritises the ability of a subject to *regain* data privacy lost online (potentially through their own initial act of publication), rather than to *expect* privacy in the first place.

F. The goals of Article 8 protection as defined by the ECtHR's reasonable expectation of privacy test in comparison to the aims of the right to be forgotten

Despite the abovementioned differences between Strasbourg's REP test and Article 17, comparisons can be made between the mutual goals of both. The ECtHR has made reference to the fact that the REP test is rooted in ensuring personal autonomy, the Court in *Pretty v United Kingdom*[477] expounding that what encompasses one's private life is an amorphous term lacking a strict definition, but the 'notion of personal autonomy is an important principle underlying the interpretation of its guarantees'.[478] Bulak and Zysset comment that the Strasbourg Court's operation of personal autonomy as a key goal of the ECHR differs between cases, but it appears that the more significant an infringement of individual autonomy is, the greater 'scrutiny' the ECtHR will engage in regarding potential violations of

[474] In all of the following cases the press made personal information known without consent: *Lillo-Stenberg, Von Hannover, Von Hannover (no.2)* and *Von Hannover (no.3)* among many other cases.
[475] *Peck, PG and JH* and *Perry* all above, n 451.
[476] *GDPR*, Article 17(1)(b).
[477] *Pretty v United Kingdom* App no 2346/02 (ECHR, 29 April 2002).
[478] Mowbray above, n 452 at 510 quoting *Pretty*, ibid [61].

Article 8 rights.[479] This in turn links back to theoretical definitions of privacy discussed in chapter 2 of this thesis. A 'privacy-as-control' definition of the right stresses the importance of individuals being able to control (to an extent) who observes them or gains information about them at a particular time.[480] It has been argued earlier in this thesis that one of the central purposes of the GDPR is to increase the amount of personal autonomy a data subject has over their private information by affording individuals greater control over dissemination of their personal data.[481] As discussed in the introduction, this reform is necessary in order to combat the 'perfect recall' capabilities of the internet and the free availability of decontextualized personal data online damaging personality rights. From the above analysis, it appears that some aspects of the ECtHR's perception relating to the goals of Article 8 protection fit harmoniously with the intended effects of the GDPR.

I. The likelihood of a 'strict' application of Strasbourg's REP test to the right to be forgotten

The direct application of Strasbourg's REP test to certain claims which could be brought under Article 17 (in particular in a scenario where a data subject uploads personal data to a publicly accessible website and subsequently wishes for the information to be deleted from third party sites) would yield unduly rigid results – as it appears that in such a scenario a data subject would not have a REP. It would be implausible of the English courts to utilise the REP test as a threshold requirement in order to invoke the right to be forgotten as this would rid the right of a significant part of its ability to reinstate informational control for web users online, as it would disallow data subjects the ability to subsequently withdraw consent to the previous processing of personal data (an ability enshrined within Article 17(1)(b)).[482] This would in fact, contradict the terms of Article 17. However, the test itself is not without relevance, as the Strasbourg court has emphasised in recent caselaw that the processing of personal data is something which may give rise to an REP. It also appears that the GDPR and

[479] Begüm Bulak and Alain Zysset, '"Personal autonomy" and "democratic society" at the European Court of Human Rights: Friends or foes?' (2013) *UCL Journal of Law and Jurisprudence* 231, 235.
[480] Jeffrey Reiman, 'Privacy, Intimacy and Personhood' (1976) 6(1) Philosophy & Public Affairs 26, Charles Fried, 'Privacy' (1967) 77 Yale Law Journal 475, Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2009), Alan Westin, 'The Origins of Modern Claims to Privacy' in Ferdinand Schoeman (ed) *Philosophical Dimensions of Privacy* (1984 Cambridge University Press) and Nicole Moreham, 'Privacy in the Common Law' (2005) 121 Law Quarterly Review 628.
[481] See Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (22 January 2012) available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (last accessed 13/4/16).
[482] *GDPR*, Article 17(1)(b).

the REP test both share the mutual goal of *protecting personal autonomy* (be it to greater or lesser degrees).

Marsoof aptly observes that 'in the context of social networking websites, it is also important to consider whether a "reasonable expectation of privacy" as perceived in relation to the traditional world could be maintained. Since social networking websites are tools made for the sharing of information, the privacy rights of social networking websites users must be considered in this light.'[483] It is important to bear this in mind for the following analysis of Strasbourg Article 8 caselaw and Article 17; although Strasbourg's REP test is highly instructive with regards to privacy rights, many of these cases concern 'traditional media' publications – therefore, arguments with regards to how the REP test relates to Article 17 may have to be nuanced with this in mind.

G. An analysis of the ECtHR's balancing factors going to the weight of the Article 8 claim and their application to the right to be forgotten

This chapter will now consider various factors that the Strasbourg Court employs in order to establish the *existence* of a REP and then to decide the *strength* of an Article 8 claim – these factors' potential influence on the interpretation of Article 17 will be critically evaluated.

I. The intimate content of the disclosed information

The ECtHR has previously held that there can be a REP with respect to bodily integrity,[484] sexuality,[485] family grief,[486] personal identity[487] and personal information.[488] Furthermore, the Court has consistently held that the more intimate the personal data disclosed, the stronger an Article 8 claim will be (and therefore increasingly likely to prevail over a competing free speech claim under Article 10).[489] An individual's sexual or romantic life is viewed by the

[483] Althaf Marsoof, 'Online social networking and the right to privacy: the conflicting rights of privacy and expression' (2011) 19(2) *International Journal of Law and Information* 110, 128.
[484] *X and Y v The Netherlands* App no 8978/80 (ECHR, 26 March 1985) and see Lorenc Danaj and Aleks Prifti, 'Respect for privacy from the Strasbourg perspective' (2012) 5 *Academicus – International Scientific Journal* 108, 112.
[485] *A.D.T v United Kingdom* App no 35765/97 (ECHR, 21 July 2000) and ibid Danaj and Prifti, 112.
[486] *Pannullo and Forte v France* App no 37794/97(ECHR, 30 October 2001) and ibid Danaj and Prifti.
[487] *Van Kück v Germany* App no 35968/97 (ECHR, 12 June 2003) and ibid Danaj and Prifti.
[488] *Smirnova v Russia* App nos 46133/99 and 48183/99 (ECHR, 24 July 2003) and ibid Danaj and Prifti.
[489] See *Von Hannover (no.2)* and *Von Hannover v Germany (no.3)*.

court as particularly sensitive and therefore peculiarly deserving of Article 8 protection – Strasbourg recognises an individual's sexuality as an important aspect of their private life.[490] This was demonstrated in the case of *Avram and Other v Moldova*, in which five women (three of whom were journalists) were secretly filmed by the police frolicking in a sauna with male police officers. The women were partially dressed, kissing the men and performing sensual dances. This footage was later passed to local television stations and broadcasted. The women claimed that the taping and dissemination of the video was in breach of Article 8 and the Strasbourg Court concurred, stating that Article 8 rights encompass an individual's sexual and romantic life which should be engaged in private, free from the observance of others.[491] It appears likely from the high frequency of this balancing principle as referred to in Strasbourg caselaw that the English (and perhaps other European) courts may also invoke this principle when balancing privacy rights under Article 17 against its freedom of expression exception.[492]

i. Application of the 'intimacy of information' factor as a balancing principle in relation to potential claims brought under the right to be forgotten

An uncertainty relating to the operation of this balancing principle is the definition of 'intimate information'. As noted in chapter 2, what one considers intimate is partly subjective, depending upon factors such as (but not limited to) culture, religion, gender, age and personality type.[493] The notion of intimacy operates as a sliding scale – for example, the ECtHR typically views data concerning an individual's sexual or romantic life as peculiarly intimate, yet in *Sæther v. Norway* the court held that a wedding was not necessarily an exclusively intimate affair – possibly as marriages are legally recorded and a public declaration of a commitment.[494]

[490] For example see *Dudgeon v United Kingdom* App no 7525/76 (ECHR, 22 October 1981) and Gómez-Arostegui above, n 447 at 6.
[491] *Avram and Other v Moldova* App no 41588/05 (ECHR, 5 July 2011) hereafter '*Avram*' and see Dirk Voorhoof, 'European Court of Human Rights: Avram and other v Moldova' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2012-1/1).
[492] Roger Toulson, 'Freedom of Expression and Privacy' (2007) 41 (2) The Law Teacher 139, 151.
[493] Chris Hunt, 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort' (2011) 37(1) Queen's Law Journal 167, 197 – 200. It must also be noted that there are certain acts which almost everyone views as intimate, such as having sex or going to the toilet.
[494] *Lillo-Stenberg* [37].

Despite the fact that intimacy is not a stipulated requirement to invoke the right to be forgotten, the GDPR's framework does give an indication towards what type of data may be considered particularly sensitive – and whether data is sensitive remains an important consideration in determining whether personal data can be lawfully processed. As earlier discussed, Article 9 of the GDPR relates to the processing of 'special categories of personal data' and imposes restrictions upon when certain categories of data can be processed:

> (1) 'Processing of personal data revealing **racial or ethnic origin**, **political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data** for the purpose of uniquely identifying a natural person, data concerning **health or data concerning a natural person's sex life or sexual orientation** shall be prohibited.'[495]

It is argued that if the English courts are to take inspiration from Strasbourg and utilise this balancing factor when interpreting the scope of the right to be forgotten, whether data is 'sensitive' should not always be determinative of whether it is seen as intimate. This would be unduly restrictive and hamper judicial flexibility when assessing unusual or complex claims under the right to erasure. The first delisting-style case in the English courts, *NT1 and NT2,* concerned hyperlinks to what has been classed as 'sensitive personal data' under section 2(g) of the Data Protection Act 1998: 'the commission or alleged commission…of any offence.'[496] Lord Justice Warby in the case held that despite the data being classed as sensitive under the 1998 Act, the content of the information was not particularly private in nature as the claimant's criminal conviction was in the public domain.[497] This serves to show that although the courts will likely consider intimacy or sensitivity of personal data during an Article 17 claim, it may not always act as a *definitive* balancing factor in a privacy-expression assessment. As Lord Justice Warby noted in the case, 'sensitive' does not necessarily mean private.[498]

Hence courts should employ an objective-subjective test, relying upon a mixture of objective cultural and subjective contextual factors.[499] Objective factors would include an examination

[495] *GDPR*, Article (1) [emphasis added].
[496] *The Data Protection Act 1998, Google Spain* and *NT1 and NT2* [139].
[497] *NT1 and NT2* [139].
[498] *NT1 and NT2* [140].
[499] Chris Hunt advocates this approach to adjudicating privacy claims in his article above at 493.

of what information may normally be considered intimate for someone of the same age or religion, whereas an examination of a subject's personal sensitivities would be specific to the individual – for example, if the data subject has had gender reassignment surgery, the subject may be particularly sensitive to a preoperative photograph circulated of themselves as a different gender. Indeed, Hunt argues that what data is considered intimate must be taken within context using 'community norms' as well as attention paid to whether a person is 'acutely sensitive' about a particular matter.[500]

Finally, if one views the intimacy of personal data balancing principle through the lens of privacy as ensuring individual autonomy, this requires that the *harm to an individual's dignity* of the personal data as publicly accessible online should be a consideration of the courts in reconciling competing claims to privacy under Article 17 and free expression. The intimacy of the personal data in question correlates to the amount of reputational harm that the public accessibility of the data is likely to cause.[501]

To conclude, this factor may indeed be useful in relation to the English courts' adjudication of competing privacy and speech rights under Article 17 (when a right to erasure conflicts with a data controller's attempted reliance upon the Article's exception relating to freedom of expression or journalism exemption).[502] In employing this balancing principle, the courts should seek to adopt an objective-subjective test in order to undertake a thorough assessment of what constitutes intimate information. Consideration of the harm done to a data subject's reputation and dignity rendered by public access to the intimate personal data should also be given by the courts.

II. The form in which the information is disclosed

When assessing the strength of Article 8 claims the ECtHR takes into account the form in which the personal data is disclosed – be it a photograph, sound recording or written text.[503]

[500] Ibid, 197-199.
[501] See Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89(3) *The Yale Law Journal* 421, 457, Robert Post, 'Three Concepts of Privacy' (2000) 89 *The Georgetown Law Journal* 2087, Robert Gerstein, 'Intimacy and Privacy' in Ferdinand Schoeman (Ed) *Philosophical Dimensions of Privacy* (Cambridge University Press 1984), 266, 270 and David Hughes, 'Two concepts of privacy' (2015) 31 *Computer Law & Security Review* 527, 534.
[502] *GDPR*, Article 17(3)(a).
[503] See Gomery above, n 445 at 427.

Indeed, it appears that 'privacy may be thought of as being domain specific.'[504] The Strasbourg Court has deemed privacy rights pertaining to photographs as particularly significant, Gomery observing that 'it has become plain that the courts treat *images* of a person in a public space differently than they would a *description* of the person in the same place.'[505] He argues that the Court justifies its prioritisation of the protection of images over text as, in a photograph, a data subject is clearly 'identifiable.'[506] Although this may be a contributing factor to the enhanced Article 8 protection photographs receive, it is argued that the reasoning of the ECtHR is actually more nuanced. If personal data is published in the form of an image (as opposed to text) it is more likely that serious infringement of a data subject's personal dignity may occur, due to the amount of personal information about an individual that a photograph is capable of importing. In turn, the publication of an image may be capable of causing a heightened degree of damage to a data subject's reputation in comparison to the written word. Marsoof comments in relation to the case of *Douglas v Hello!* in the English courts:

> '…the unauthorised publication of photographs has been condemned more forcefully than other forms of privacy leaks. In *Douglas v Hello!* it was observed that "[a] photograph can certainly **capture every detail of a momentary event in a way which words cannot,** but a photograph can do more than that. A **personal photograph can portray, not necessarily accurately, the personality and the mood of the subject** of the photograph."'[507]

Similarly, in *Von Hannover v Germany (no.2)*, the ECtHR expounded:

> 'Regarding photos, the Court has stated that a person's image constitutes one of the **chief attributes of his or her personality**, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development'.[508]

[504] Marsoof above, n 483 at 129.
[505] Gomery above, n 445 at 427 [emphasis added].
[506] Ibid, 427.
[507] Marsoof above, n 483 at 129 and *Douglas v Hello!* [2006] QB 125, [106 – emphasis added].
[508] *Von Hannover (no.2)* [96 – emphasis added].

i. Application of the 'format of personal data disclosed' balancing factor to the interpretation of the right to be forgotten

a. A data subject wishes to exercise the right to be forgotten in relation to images depicting themselves which are accessible online

The above arguments in favour of photographs as warranting particularly strong privacy-related protection appear to be rooted within the theory that images are capable of conveying more personal information than text relating to a data subject, thereby infringing personality rights in a particularly serious way. Article 17 does not reference specific forms of personal data.[509] However, it appears likely that in practice many individuals will use the right to be forgotten to delete photographs of themselves available on webpages. It has been shown through news coverage that photographic images of individuals on the internet have the ability to detrimentally impact a person's private life as well as their career.[510] In this sense the prioritisation of Article 8 protection for photographic images by the ECtHR is to be welcomed, as public accessibility of personal information in the form of images online may have a particularly significant detrimental impact upon a data subject's reputation.

b. A data subject wishes to exercise the right to be forgotten in relation to personal data in the form of text which is accessible online

However serious a data breach in the form of photographs may be, it is argued here that other formats of personal data accessible online, including text, also have the potential to be significantly detrimental to a data subject's reputation. For example, it cannot be denied that intimate details concerning a sexual encounter that are publicly available online may be significantly damaging to a data subject's personality rights. In order for Article 17 to operate effectively it is submitted that there should not be a strict or exhaustive categorisation of the forms of data that it can be applied to. Rather, the English courts should undertake a flexible approach on a case-by-case basis when deciding what type of information should be

[509] *GDPR*.
[510] Daniel Bean, '11 Brutal Reminders That You Can and Will Get Fired for What You Post on Facebook' (*Yahoo Tech*, 6 May 2014) accessible at: https://www.yahoo.com/tech/11-brutal-reminders-that-you-can-and-will-get-fired-for-84931050659.html (last accessed 24/4/16) and also see the story of Ashley Payne mentioned in this thesis' introduction: The Daily Mail, 'Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook'(*The Daily Mail Online*, 7 February 2011) accessible at: http://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html (last accessed 24/4/16).

removed. It may be the case that the *content* of the data (and the consequences of its open accessibility on the data subject in question) as opposed to its *form* is the most important factor for the courts to focus upon when determining whether a right to be forgotten under Article 17 trumps a competing interest in freedom of expression under Article 17(3)(a) or the journalistic exemption.[511]

III. Prior conduct of the person concerned as waiving their right to privacy

The prior conduct of an individual in terms of soliciting or shunning publicity is a consideration cited by the ECtHR when evaluating the strength of Article 8 claims.[512] Indeed, in *Sæther v. Norway* the Strasbourg Court referenced 'prior conduct of the person concerned' as one of five factors that ought to be evaluated when balancing the rights of privacy and freedom of expression.[513] Furthermore, as discussed below, in *Axel Springer* and *Von Hannover v Germany (no.2)* in 2012 the ECtHR impliedly accepted the notion of a data subject *waiving* their privacy rights through previous disclosure of personal information.[514]

i. Prior conduct of an individual as strengthening their claim to privacy

There is some evidence from the caselaw that the Strasbourg Court may deem the prior conduct of an individual in *shielding* themselves from public intrusion into their private affairs as strengthening an Article 8 claim. In *Von Hannover v Germany (no.3)*, the Strasbourg Court acknowledged that Princess Caroline's lack of engagement with the press was a relevant consideration pertaining to her claim to privacy (be it considered explicitly or implicitly by the courts), Bedat observing:

> 'The Court raised the point made by the applicant that the German courts had failed to **"explicitly" consider her efforts to keep her private life out of the press, as manifested by previous legal actions**. The Court, however, found that the German

[511] *GDPR*.
[512] *Lillo-Stenberg, Von Hannover (No.2), Von Hannover* and *Axel Springer AG v Germany* App no 39954/08 (ECHR, 7 February 2012) hereafter '*Axel Springer'*.
[513] *Lillo-Stenberg* [34] and see Dirk Voorhoof, 'European Court of Human Rights: Lillo-Stenberg and Sæther v. Norway' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2014-3/1).
[514] *Axel Springer* [92] and [101], *Von Hannover v Germany (no.2)* [111] and Gavin Phillipson, 'Press freedom, the public interest and privacy' in Andrew Kenyon (Ed) *Comparative Defamation and Privacy Law* (Cambridge University Press 2016) at 151.

courts' reasoning indicated that this had been considered "**in substance".** This, the Court concluded, constituted "sufficient consideration" for the purpose of balancing the competing interests at stake.'[515]

Similarly, a consideration of the ECtHR in *Von Hannover v Germany* appeared to be that within certain images captured of Princess Caroline that she had made an effort to hide herself from the public eye. One of the photographs depicted Caroline dining in a secluded place (a corner of a restaurant) and another her relaxing within a private members' club.[516]

ii. Application of the 'prior conduct as giving rise to a heightened claim to privacy' balancing factor to the right to be forgotten

a. A data subject uploads personal data online to a restricted website, the data subsequently leaked and posted to third party sites – the 'restricted access' scenario

If this balancing factor is read across to a situation whereby an individual seeks to rely on Article 17 pertaining to personal information they have disclosed to a partially restricted website (for example, data which can only be viewed by approved 'friends' on Facebook), it could be argued that this constitutes *prior conduct indicating the desire for a degree of privacy* in respect of the information. Therefore, under the Strasbourg Court's reasoning, the individual's prior conduct may give rise to a heightened degree of privacy-protection under Article 8.

b. A data subject uploads personal data to an unrestricted and publicly accessible website – the 'personal public disclosure' scenario

However, this factor cannot be similarly read across to aid a claimant in a balancing exercise in the situation where an individual has uploaded personal data to a publicly accessible online domain, and subsequently wishes to rescind publication.[517] Here, rather than an individual's

[515] Alexia Bedat, 'Case Law, Strasbourg; Von Hannover v Germany (no.3) Glossing Over Privacy' (*Inforrm Blog*, 13 October 2013), emphasis added; available at: https://inforrm.wordpress.com/2013/10/13/case-law-strasbourg-von-hannover-v-germany-no-3-glossing-over-privacy-alexia-bedat/ and *Von Hannover (no.3)* [55].
[516] *Von Hannover* [68 and 74] and Mowbray above, n 452 at 581.
[517] Article 17(1)(b) allows a data subject to subsequently withdraw previously given consent to processing.

prior conduct indicating a wish to retain (partial) privacy in respect of the information, the individual has conversely demonstrated an initial willingness to make their personal information freely available.

iii. Prior conduct of an individual amounting to a waiver of privacy rights

The ability of an individual (in particular, a celebrity) to waive their right to privacy through their previous solicitation of publicity has been acknowledged by the English courts for some time. The case of *Theakston v MGN* concerned the publication of photographs of television presenter Jamie Theakston taken inside a brothel.[518] Mr Justice Ouseley argued that, as Theakston 'has **courted publicity**…and not complained at it when, hitherto, it has been very largely favourable to him…**he cannot complain if publicity given to his sexual activities is less favourable in this case**.'[519] Similarly, in *Axel Springer* the ECtHR found that the prior conduct of the person concerned must be taken into consideration when assessing the weight of a claim under Article 8, observing:

> 'The **conduct of the person concerned prior to publication of the report** or the fact that the photo and the related information have already appeared in an earlier publication are also factors to be taken into consideration…However, **the mere fact of having cooperated with the press on previous occasions cannot serve as an argument for depriving the party concerned of all protection against publication of the report or photo at issue**.'[520]

The court's statement that previous conduct of an individual amounting to solicitation of the press would not deprive a data subject of *all* privacy rights implies that such conduct would act to *partially* reduce access to privacy rights. As Phillipson notes, this statement of the court is 'of little comfort to privacy advocates' as it merely indicates that waiver cannot operate to negate a right to privacy in its entirety.[521] Furthermore, the Strasbourg Court held that as the

[518] *Theakston v MGN Limited* [2002] EWHC 137, [2002] E.M.L.R 22.
[519] Ibid, [68 – emphasis added].
[520] *Axel Springer* [92, emphasis added] also see Sara Mansoori, 'Case Law: Axel Springer v Germany, Grand Chamber finds violation of Article 10' (*Inforrm*, 9 February 2012) available at: https://inforrm.wordpress.com/2012/02/09/case-law-axel-springer-v-germany-grand-chamber-finds-violation-of-article-10-sara-mansoori/ (last accessed 1/5/16).
[521] Phillipson above, n 514 at 151.

data subject, a German television actor, had previously given interviews and in doing so revealed certain details about his personal life, his reasonable expectation of privacy (and in turn the strength of a claim he could bring under Article 8) had been reduced. The Court stated:

> 'He had himself revealed details about his private life in a number of interviews…In the Court's view, he had therefore **actively sought the limelight**, so that, having regard to the degree to which he was known to the public, his **"legitimate expectation"** that his private life would be effectively protected was **henceforth reduced**.'[522]

As Phillipson observes, the Court did not elaborate upon precisely why the claimant's choice to reveal certain select details about his personal life led to his reasonable expectation of privacy being reduced with respect to other personal data which he had *not* voluntarily disclosed.[523] Regardless of the criticism that this judgment has received, it shows a clear acceptance of an implied waiver of privacy rights by the Strasbourg court.

iv. How the balancing factor of prior conduct (waiver) can be applied to the right to be forgotten

a. A data subject has uploaded publicly accessible personal data about themselves online

Using the reasoning of the English and Strasbourg courts that some *voluntary* disclosure of personal data may result in a data subject forgoing the right to privacy in relation to subsequent *involuntary* disclosures, it would appear that a data subject who has initially uploaded personal information to an openly accessible platform online and subsequently wishes to rescind the information has, at least partially, waived their right to privacy. If this principle were to be directly read across by the European courts to the right to be forgotten it would drastically reduce its practical effect, as it is likely that in some circumstances data requested for deletion may have been previously uploaded by the data subject in question – potentially when they were significantly younger or at a different stage of their life in terms of romance or career. They may now have good reason to want to delete the information; it

[522] *Axel Springer* [101 – emphasis added].
[523] Phillipson above, n 514 at 150 - 1.

may no longer be fitting to an individual's online image to have past pictures of themselves behaving raucously at university parties accessible online if they are seeking employment at a professional establishment.[524] Application of waiver in this way would fundamentally conflict with the operation of Article 17(1)(b) as giving data subjects an opportunity to subsequently *withdraw* consent to data processing.[525]

b. A data subject wishes to delete personal data uploaded about themselves by a third party without consent

A potentially extremely broad reading of waiver could be adopted by the English or European courts in a situation whereby personal data concerning a data subject has been disclosed online (without consent) by a third party and a data subject is deemed to have partially waived their right to privacy by virtue of *previously voluntarily* disclosing different personal information online (perhaps on their own social networking webpage). However, using waiver in this way would plainly conflict with the right to privacy as informational autonomy – in other words, the ability of an individual to disclose what information they choose, to whom they choose, when they choose.[526] Phillipson cogently argues that 'the notion that a voluntary disclosure of private information prevents an individual from being able to complain about an involuntary disclosure is *wholly incompatible* with the core privacy value of the individual's right to control over the release of personal information.'[527]As discussed in Chapter 2, making such choices is a fundamental facet of an individual exercising privacy.[528] These choices allow for personal development, as an individual is given control over how and to what degree they are perceived by others. The decision to disclose certain types of information to particular individuals allows someone to adopt different 'faces' in society and maintain specific types of relationships; for example, a person may feel comfortable discussing sexual encounters with their best friend but perhaps not their manager at work. As Rachels and Fried observe, an individual's voluntary restriction of select pieces of information and voluntary disclosure of others is wholly authentic.[529] The notion of waiver

[524] See Alan Henry, 'How You're Unknowingly Embarrassing Yourself Online (and How to Stop)' (*LifeHacker*, 5 October 2013) accessible at: http://lifehacker.com/how-youre-embarrassing-yourself-online-without-knowing-495859415 (last accessed 1/5/16) and Solove above, n 203 at 17.
[525] *GDPR.*
[526] Phillipson above, n 514 at 150.
[527] Ibid, 150.
[528] Nissenbaum and Reiman above, n 480.
[529] Charles Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475, James Rachels, 'Why Privacy is Important' (1975) 4(4) *Philosophy & Public Affairs* 323 and Westin above, n 480

inhibits an individual's exercise of choice over what personal data remains private or is made public, instead dictating that if *some* personal data has voluntarily been disclosed by data subject in the past, a data subject – at least in part – forfeits their right to restrict access to personal data in the future. It is therefore argued that the notion of a waiver of privacy rights through prior conduct should not be utilised by the English courts when interpreting the scope of the right to be forgotten.

IV. Circumstances within which the personal information was obtained

The ECtHR has stated that the circumstances in which personal data is obtained and reported is a principle potentially giving weight to an Article 8 claim and its subsequent balance against Article 10 rights. In *Sæther v. Norway*, the Strasbourg Court emphasised the relevance to the REP test of the way in which intrusive photographs were captured, commenting, 'the situation would have been different if the photographs had been of events taking place in a closed area, where the subjects had reason to believe that they were unobserved.'[530] Indeed, a claimant's lack of knowledge that intrusive photographs had been taken appears to be a factor going to the weight of an Article 8 claim.[531] In *Von Hannover v Germany*, the frequency of photographs being taken and published was also deemed to be a relevant consideration in assessing the strength of an Article 8 claim by the Strasbourg Court. The court noted that 'photos appearing in the tabloid press are often taken in a climate of *continual harassment* which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution.'[532] The court observed:

> 'In the present case this point is illustrated in particularly striking fashion by the photos taken of the applicant at the Monte Carlo Beach Club tripping over an obstacle and falling down…It appears that these photos were taken **secretly at a distance of several hundred metres**, probably from a neighbouring house, whereas **journalists' and photographers' access to the club was strictly regulated**.'[533]

[530] *Lillo-Stenberg* [39].
[531] *Von Hannover* [68].
[532] *Von Hannover* [59].
[533] *Von Hannover* [68 – emphasis added].

i. Application of the balancing factor of the 'circumstances within which private data is obtained' to the right to be forgotten:

a. A data subject has uploaded personal data online to a publicly accessible website – 'personal public disclosure' scenario

Upon first examination, this balancing factor does not appear to be easily read across to a situation where a data subject invokes the right to be forgotten in respect of personal data they have initially uploaded to a publicly accessible website and the data has subsequently been copied by third parties to other sites out of a data subject's control. As the subject has voluntarily disclosed the information to the public at large, surreptitious data-gathering does not appear to have occurred here; as under the ECtHR's reasoning, a data subject could have been expected to reasonably foresee that a third party had the ability to gather and further disseminate the data.

However, on a broader and more flexible interpretation of this factor, it could be argued (in the above scenario) that if a data subject was *unaware* of a third party taking and further disseminating private data on a *continual* basis which amounted to harassment, parallels could be drawn to the circumstances surrounding photographs captured of Princess Caroline in *Von Hannover v Germany*.[534] Despite the fact that Caroline was present in public places when the images were taken (Monte Carlo beach club and a restaurant), the fact the pictures were gathered without her knowledge and on multiple occasions gave rise to a successful Article 8 claim. Similarly, it could be argued that notwithstanding the fact a data subject has uploaded personal data to a publicly accessible website, if personal data is copied by a third party to other sites *on a continual basis* without the data subject's knowledge, this could strengthen a privacy claim.

b. A data subject uploads personal data online to a restricted website, the data subsequently leaked and posted to third party sites – the 'restricted access' scenario

[534] *Von Hannover*.

In a circumstance where a data subject uploads personal data online to a website which has partially restricted access,[535] and a user copies the data and disseminates it further to third party sites, it could be deemed, using this factor, that the data has indeed been collected in a surreptitious way. This is due to the fact that a data subject reasonably expected that the information would only be viewed by a select audience because of the restricted nature of the webpage yet the information has been circulated on a wider platform without a data subject's knowledge or consent.[536]

c. An individual wishes to exercise their right to erasure in relation to personal data initially uploaded by a third party – the 'third-party poster' scenario

It is in this situation that the 'means by which the data is gathered' factor is most easily read across in application to the right to be forgotten: in the vast majority of Strasbourg Article 8 jurisprudence personal data is initially gathered by a third party (usually the press, and often in the form of photographs) and later disseminated.[537] The difference between this scenario and the two previously discussed is that this situation does not necessarily involve voluntary disclosure of personal data by the data subject at any stage. If an individual seeks to rely on their right to erasure in respect of photographs surreptitiously taken without consent and uploaded online, this factor would indicate to the English courts (when reading this factor across) that there is a heightened strength of a right to deletion under Article 17 when balanced against the freedom of expression exception.[538]

V. Does the personal data relate to a public or private location?

Several Article 8 cases in Strasbourg jurisprudence focus on physical location with regards to the personal data in question.[539] For example, a data subject's claim to privacy in respect of a photograph taken of them in a public street is less likely to garner Article 8 protection than if they were in a private dwelling.[540] A conservative interpretation of what constitutes a private zone is evident in some aspects of the judgment of *Von Hannover v Germany*. Judge Barreto

[535] For example someone's 'friends' on Facebook or approved followers on a restricted Twitter account. See Facebook.com, accessible at: https://en-gb.facebook.com/ and Twitter.com, accessible at: https://twitter.com/?lang=en-gb (last accessed 2/5/16).
[536] See *Von Hannover* [68] and *Peck* above, n 451.
[537] As was the case in *Von Hannover Nos. 1, 2* and *3* as well as *Lillo-Stenberg.*
[538] *GDPR,* Article 17(3)(a).
[539] See for example *Von Hannover, Von Hannover (no.2)* and *Peck* above, n 451.
[540] See *Lillo-Stenberg and Sæther v. Norway* App no 13258/09 (ECHR, 16 January 2014).

sought to argue that Princess Caroline's Article 8 claim with respect to photographs of herself published in a German magazine was weak, as several images depicted Caroline in places accessible to the general public.[541] Similarly, *Sæther v. Norway* concerned a wedding of a celebrity couple who had married outdoors on a publicly accessible islet.[542] An article had been published about the couple's wedding along with several photographs of the ceremony, captured by paparazzi stationed near the wedding using strong-lensed cameras. The ECtHR upheld the Icelandic Court's judgment that Article 10 interests should prevail over the couple's Article 8 claim to bar publication of the photos, as it was an outdoor wedding in a public place (and holiday destination).[543]

i. Application of this factor to potential Article 17 claims:

a. Information concerning a data subject ('A') is uploaded by a third party ('B') without A's consent – third party-poster scenario

Under a conservative reading of this balancing factor, the English courts would be more likely to order that erasure under the GDPR prevails over its free expression exception[544] if the image or text related to an activity undertaken by the data subject in a physically private location.[545]

b. A data subject (A) has voluntarily made personal data available online concerning themselves and this data has been reposted to third party sites (controlled by 'C') – the 'personal public disclosure' scenario

It could be argued that data disseminated online to a restricted website[546] is in a private *virtual location* due to its limited access. Therefore, according to this balancing factor, this may warrant privacy-protection under Article 17. However, this conservative line of reasoning leads to the conclusion that personal data posted online by a data subject which is

[541] Gómez-Arostegui above, n 447 and *Von Hannover*.
[542] *Lillo-Stenberg*.
[543] See Dirk Voorhoof, 'European Court of Human Rights: Lillo-Stenberg and Sæther v. Norway' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2014-3/1).
[544] *GDPR*, Article 17(3)(a).
[545] As was stated in the case in *Von Hannover*.
[546] For example a 'protected' tweet on Twitter. See: Twitter, 'About Public and Protected Tweets' available at: https://support.twitter.com/articles/14016 (last accessed 22/4/16).

in a publicly accessible virtual location (absent of viewing restrictions) *does not* warrant protection under Article 17.

It is submitted that this is an unduly restrictive interpretation of the right to be forgotten and if the English courts adopt such a position, this will negate most of the impact that the right to erasure will have on personality rights. Individuals are *more likely* to wish to rescind publication of publicly accessible personal data online due to its wide readership. It seems logical that the majority of individuals who will invoke the right to erasure will do so in order to regain control of their online image, in fear of their reputation being tarnished. Indeed, academics such as Solove have observed that there is a growing rise in the number of people hiring private companies to 'clean up' their online persona by attempting to curtail the amount of freely accessible personal data relating to themselves online.[547] Furthermore, the line between what information is truly public or private in a virtual location online is somewhat blurred due to the varying degrees of accessibility to data online. If an individual posts personal data to a seldom-frequented part of the web and the information subsequently becomes 'viral' (in other words, is widely and quickly disseminated by others) it is unclear whether this data was initially part of the private or public domain, as it was (at first) only viewed by a limited number of internet users.[548] Similarly, if a data subject uploads personal information anonymously to an openly accessible website to be later identified, it is uncertain whether this should be deemed part of a public or a private virtual zone – as although the user's data was open to the public, their identity was initially private.[549] For the abovementioned reasons, it is concluded that applying a restrictive reading of 'physically public location' balancing factor to the interpretation of Article 17 would be punitive for data subjects – as if any personal data was disclosed as freely accessible online, such a reading would view it as 'fair game' for further dissemination.

Helpfully, there is evidence that the Strasbourg Court is adopting an increasingly nuanced approach towards what information is contained within a public or a private zone, seemingly linked to an individual's emotionality or state of mind. Indeed, in the case of *Pfeifer v Austria* the ECtHR stated that Article 8 encompasses 'a person's physical and psychological

[547] See Solove above, n 203. It is also important to note that the protection of an individual's reputation is an aspect of Article 8 rights, confirmed in numerous ECtHR cases such as *Sipos v Romania* App no 26125/04 (ECHR, 3 May 2011). Also see *NT1 and NT2*.
[548] The trend of seemingly banal or mildly amusing data becoming viral overnight is increasingly prevalent in the digital age.
[549]See *The Author of a Blog v Times Newspapers Ltd* [2009] EWHC 1358 (QB).

integrity.'[550] When attempting to define the scope of the right to privacy in *Niemietz v Germany*, the court expounded that 'it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world,'[551] seemingly advocating a flexible reading of what a private zone could encompass.[552] However, Strasbourg's breakthrough case with regards to the expanding notion of what personal information may be contained within an individual's private sphere is the seminal *Von Hannover v Germany*.[553] The Court here observed that there is 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".'[554] This sentiment was echoed in the more recent case of *Avram and Other v Moldova*.[555] In *Von Hannover,* Princess Caroline of Monaco sought to suppress publication of photographs of herself in a German magazine. The images depicted, among other things, the Princess running errands with her children, relaxing on a beach in a swimsuit and dining with a male companion.[556] The Princess applied to the German Constitutional Court (hereafter 'GCC') for an injunction to stop the photographs' publication. The GCC stated that because the photographs had been taken in a *physically public location* (and that Caroline was a public figure)[557] that she must tolerate publication of the photographs. The GCC held that the only photographs which gave rise to privacy-related protection were those which contained images of her children or were of Caroline in a 'secluded place.'[558] However, the ECtHR disagreed and expounded that the 'secluded place' test employed by the GCC was unacceptably narrow. The Strasbourg court decided that despite the fact the images depicted Princess Caroline in a public place they were deserving of protection under Article 8 as they gave viewers an insight into her personality and 'psychological integrity.'[559]Toulson notes that the ECtHR's use of the seclusion requirement is complicated. The modern and progressive formulation of the factor appears to relate to

[550] *Pfeifer v Austria* App no 24733/04 (ECHR, 17 February 2011) hereafter '*Pfeifer*' and Bulak and Zysset above, n 479 at 234.
[551] *Niemietz v Germany* App no 13710/88 (ECHR, 16 December 1992) [29] and Mowbray above, n 452 at 486.
[552] It is important to note that this approach potentially conflicts with the majority's viewpoint in *Campbell* that some information is 'obviously private' – see Nicole Moreham, 'Privacy in the Common Law' (2005) 121 *Law Quarterly Review* 628, 646.
[553] *Von Hannover.*
[554] Ibid [50].
[555] *Avram* [37].
[556] *Von Hannover.*
[557] This will be discussed in detail in a later section of this chapter.
[558] *Von Hannover* and Bryce Newell, 'Public Places, Private Lives: Balancing privacy and freedom of expression in the United Kingdom' (2014) (77th ASIS & T Annual Meeting) Available at: SSRN: http://ssrn.com/abstract=2479093 (last accessed 22/4/16) 6.
[559] Ibid.

what the data in question *reveals* about an individual's private life rather than whether the photographs were actually taken in a public location.[560]

This nuanced approach to the *physically public location* balancing factor demonstrated by the Strasbourg Court above can potentially be applied to data dissemination scenarios whereby a data subject has uploaded information about *themselves* (the data subsequently posted to third party sites out of their control) or a *third party* has initially uploaded the personal data. According to the reasoning of the Strasbourg court in *Von Hannover v Germany*, the data may warrant privacy-protection if it gave those who witnessed it online an 'insight' into the data subject's personality. This analytical approach to balancing the rights of privacy and free expression could be adopted by English courts regardless of who initially disseminated the data. Gomery argues that in *Von Hannover* that the ECtHR adopted an approach that could be called "privacy as autonomy" as the court's attention was focused upon the 'claimant's autonomy in the particular circumstances of the case at hand.'[561] He observes:

> 'privacy as autonomy falls squarely within the long liberal tradition in which individual autonomy has been recognised as a goal of the enlightened political community…[it is] a moral and philosophical concept to which the courts may point in the development of the law and recognition of legal rights.'[562]

Indeed, Gomery advocates that, contrary to the approach of the German Constitutional Court, 'privacy is more than seclusion.'[563] It is submitted that it is essential when applying the *public location* balancing factor to potential claims brought under the right to erasure that the notion of 'private zone' is not taken unduly conservatively or literally. Rather, a nuanced approach with a focus upon a data subject's psychological integrity as demonstrated in *Von Hannover v Germany* ought to be adopted. Otherwise, individuals may be forced to seclude themselves (both virtually online and physically in everyday living), constraining their behaviour and life choices for fear of their actions being recorded and documented online indefinitely.[564]

[560] Toulson above, n 492 at 140.
[561] Gomery above, n 445 at 409.
[562] Ibid, 409 [emphasis added].
[563] Ibid.
[564] See Westin, above n 480 at 56, Francis Chlapowski, 'The Constitutional Protection of Informational Privacy' (1991) 71 *Boston University Law Review* 133, Tom Gerety, 'Redefining Privacy' (1977) 12(2) *Harvard Civil Rights-Civil Liberties Law Review* 233, 281, Ruth Gavison, 'Too Early for a Requiem? Warren and Brandeis Were Right on Privacy Vs. Free Speech' (1992) 43(3) *South Carolina Law Review* 437, Julie Cohen, 'What Privacy is For' (2013) 126 *Harvard Law Review* 1904, 1918-20 and Gerstein above, n 501 at 266.

Theoretical as well as substantive informational autonomy is therefore at risk if increased data privacy protection is not afforded by the Article 17. Furthermore, a flexible and context-driven approach should be undertaken in applying the ECtHR's metaphorical discourse of spheres of privacy to the interpretation of Article 17. An 'intense focus on the facts'[565] is required if the English courts utilise this principle to balance the competing rights of privacy and speech in relation to Article 17, as what is part of an individual's public or private domain is inherently context-dependent and therefore subjective.[566]

It is concluded from this section that the conservative or physical notion of what constitutes information in the public or private domain is out-dated in its application to the right to be forgotten, particularly regarding the lack of clarity pertaining to what constitutes the public domain online. If the English courts are to use this balancing principle in interpreting the scope of Article 17 they must take influence from the more nuanced approach to this principle adopted by the ECtHR in cases such as *Avram* and *Von Hannover v Germany*, with a focus upon *what the data in question reveals* about the psychological integrity of the data subject.[567] In order to do this, the extent of the restriction upon a data subject's theoretical or substantive autonomy due to the availability of this information online must be examined.

VI. When the personal data relates to a public figure or a celebrity[568]

The Strasbourg court has held that, *in certain circumstances*, celebrities or famous figures do have a right to privacy. In *Sæther v. Norway* the ECtHR commented upon the position of celebrities with regards to Article 8 claims, stating that:

> 'The Court also reiterates that, in certain circumstances, **even where a person is known to the general public,** he or she may rely on a **"legitimate expectation" of protection of and respect for his or her private life**…' [569]

Conversely (and confusingly), it appears that the Strasbourg court does also find that a person's celebrity status can give weight to a competing Article 10 claim – and weaken their

[565] Toulson above, n 492 at 150.
[566] Gomery above, n 445 at 417.
[567] *Von Hannover* and *Avram.*
[568] The issue of claimants as well-known figures will also be touched on in chapter 5 of this thesis.
[569] *Lillo-Stenberg* [97 – emphasis added].

Article 8 claim. In *Von Hannover v Germany (no.2)* the ECtHR found that it did not violate Princess Caroline of Monaco's Article 8 rights to publish a photograph of her alongside an article (concerning Monaco), because Caroline was a public figure.[570] Furthermore, despite Strasbourg's abovementioned comments in *Sæther v Norway*, the court ultimately found that the couple in question did not have a right to privacy in respect of covert photographs taken of their wedding - the fact the couple were celebrities contributed to this finding.[571] The court has stated celebrities and public figures do not have *the same* right to claim protection over their private life as wholly private citizens:

> 'whilst a private individual unknown to the public may claim particular protection of his or her right to private life, the same is not true of public figures…'[572]

This continued position of the Strasbourg Court has been criticised by Hughes, who notes that theoretical justifications for shielding the privacy of private individuals can be applied in the same way to public figures – and there is no robust theoretical standpoint to treat the privacy rights of celebrities and private citizens differently.[573] Although the ECtHR makes it clear that there are certain limitations on privacy that a public figure or a celebrity will experience, these limitations are far from absolute; both the Grand Chamber judgments of *Couderc v France* and *Von Hannover (No.2)* have stated that public figures can still, in some circumstances have a 'limited expectation' of privacy.[574] The case of *Couderc* concerned news outlets that had published a story concerning the lovechild of Prince Albert of Monaco. The Prince took the French company that had broken the story to court in France, the national court fining the outlet and ordering it to publicly redact the story. The publishers took the case to Strasbourg, arguing that their Article 10 rights had been infringed and ultimately won their case; however, that is not the notable aspect of the decision. Despite the fact that expression in this case triumphed, the Court acknowledged that there were aspects of a

[570] *Von Hannover (No.2)* and see Dirk Voorhoof, 'European Court of Human Rights: Axel Springer AG v. Germany' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2012-3/1).
[571] *Lillo-Stenberg* and see Dirk Voorhoof, 'European Court of Human Rights: Lillo-Stenberg and Sæther v. Norway' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2014-3/1).
[572] *Couderc and Hachette Filipacchi Associes v France* App no 40454/07 (ECHR, 12 June 2014) [84].
[573] Kirsty Hughes, 'The Public Figure Doctrine and the Right to Privacy' (2019) 78(1) *Cambridge Law Journal* 70, 71.
[574] *Couderc* above n 572 at [84] and *Von Hannover (No.2)* [97].

famous person's life that could still be protected under Article 8, and that public interest value of the information must be *legitimate*, and not solely serve to satisfy public curiosity.[575]

In summary, the fact that a claimant is well-known will not always stop them successfully claiming for an invasion of privacy under the ECHR, but it will likely weaken their case during the balancing exercise the Court conducts between Articles 8 and 10. Hughes has observed that awarding celebrities privacy rights has been deemed 'highly controversial' and both the English and the Strasbourg courts have attracted criticism from the media on the basis that this is 'oppressive'[576] and detrimental to reportage. What will tip the balance for or against the celebrity's Article 8 claim is the presence of other factors in the case. The Grand Chamber in *Couderc* gives the example of an intimate photograph of a celebrity as published; despite the fact that a person is famous, they may still have a right to privacy in respect of the picture as 'a photograph may contain very personal or even intimate "information" about an individual or his or her family'.[577]Manner in which the information is obtained is also crucial to these types of cases – a celebrity is more likely than a private individual to be repeatedly followed and harassed, and if this is present this can also aid their privacy claim.[578] The court also stated that *extent* to which a person is well known is a relevant factor.[579]

The Grand Chamber in *Couderc* also makes the point at length that private information about the sex lives of public figures, even if they are particularly high profiles ones (such as Prime Ministers) is particularly protected.[580] After citing some exceptions to this rule,[581] the Court posited:

> '[a] **person's romantic relationships are, in principle, a strictly private matter**. It follows that, in general, details concerning a couple's sex life or intimate relations

[575] Ibid *Couderc* [107] and Clare Overman, Couderc and Hachette Filipacchi Associés v. France: A New "Respect" for Private Life? (*Oxford Human Rights Hub*, 23 November 2015) accessible at: http://ohrh.law.ox.ac.uk/couderc-and-hachette-filipacchi-associes-v-france-a-new-respect-for-private-life/ (last accessed 2/7/19).
[576] Hughes above n 573, 70-71.
[577] *Couderc* above n 572 at [85] and also see the 'format' Article 8 factor earlier in this chapter.
[578] Ibid *Couderc* [86] and *Von Hannover* [68].
[579] Ibid *Couderc* [117].
[580] Ibid [99-102].
[581] See *Ojala and Etukeno Oy v. Finland*, App no 69939/10 (ECHR, 14 January 2014) [54-55] and *Ruusunen v. Finland*, App no 73579/10 (ECHR, 14 January 2014) [49-50]. The Court cited these cases as exceptions to the rule, given that disclosing details about the intimate relationships of public figures in these instances was necessary as it revealed important personality traits of the leaders concerned – including dishonesty.

> should only be permitted to be brought to the public's knowledge without prior consent in exceptional circumstances.'[582]

The court here, then, makes it clear that 'voyeurism' is not enough to justify the publication of facts about a person's private life, even if they are famous;[583] some better reason needs to be adduced. [584] In the case of *Couderc*, the reason was the right of the public to know about the birth to the Prince of a child at the time when he was thought to be 'single and childless' and this was enough to tip the balance in favour of Article 10. The Court reasoned that this could have implications on the royal family of Monaco, the line of succession and how they relate to the public at large.[585] This does seem consistent with the ECtHR's position with regards to the decision of *Von Hannover (No.2)* and the statement of the court that the public had a right to know about the failing health of Prince Rainier.[586]

A further crucial consideration is the particular 'role' or 'function' that the person in question has, and whether the private information in question relates to this role – and whether it is important that the public is informed of some aspect of the figure's private life that relates to this function.[587] In this capacity, the press can be seen as playing the role of a 'watchdog', which is a Article 10 'balancing factor' that will be discussed in detail in the next chapter.

i. Application of the 'personal data relating to a public figure' balancing factor to the interpretation of the right to be forgotten

The point must be made that the public figure doctrine is only relevant to the right to erasure to a limited extent: it will only apply to public figures seeking to make use of the right. In giving guidance on delisting requests made after *Google Spain*, Article 29 Working Party have stated that an 'exception' to the general delisting right are requests made by public figures, in respect to information online about them that the public has an interest in

[582] *Couderc* above n 572 at [99 – emphasis added].
[583] Ibid [101-102].
[584] See the 'press as a watchdog' Article 10 balancing factor discussed in the next chapter.
[585] *Couderc* above n 572 at [109].
[586] Ibid [112] and *Von Hannover (No.2)* [38].
[587] Ibid *Couderc* at [12] and see *Krone Verlag GmbH & Co KG v. Austria*, App no 34315/96 (ECHR, 26 February 2002) [37] and *News Verlags GmbH & Co.KG v. Austria*, App no 31457/96, [54].

(particularly if it reveals improper conduct).[588] The Working Party focused the issue on whether someone 'play[s] a role' in public life.[589] Additionally, the Working Party importantly noted that *playing a role* in public life is a wider criterion than being a public figure – which seems to hint that the Working Party believe that certain people, although they may not be public figures, have certain aspects of their life in the public domain in a way which may generate public interest. Article 29 Working Party have acknowledged that this is an unclear notion:

> 'It is not possible to establish with certainty the type of role in public life an individual must have to justify public access to information about them via a search result.'[590]

It is argued that celebrities or public figures should indeed have a right to data privacy online, as the ability to keep certain aspects of one's life private is an important part of personal autonomy and human dignity which all individuals should enjoy (even the famous).[591] The ECtHR has demonstrated that it is prepared (in certain limited circumstances) to uphold Article 8 claims from public figures,[592] leading to the tentative conclusion that *it is* possible for a celebrity to successfully rely upon an erasure request under Article 17 if there is no genuine public interest in the information that the celebrity has requested for deletion. If a public interest was in fact established, according to Article 29 Working Party's above guidance, it is unlikely that a delisting request would succeed. A data controller could rely on the exception pertaining to freedom of expression in Article 17(3)(a) or the journalism exemption which may engage 'role model' arguments pertaining to celebrities; in other words, the value of distributing personal data about the misdeeds of those who are well-known.[593] What constitutes a matter of *legitimate* public interest in relation to public figures will be discussed in detail in the following chapter.

---

[588] Article 29 Working Party, 'Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12' (26 November 2014) accessible at: https://www.dataprotection.ro/servlet/ViewDocument?id=1080 (last accessed 30/7/19), 13. Also see the next chapter of this thesis – the 'press as a watchdog'.
[589] Ibid.
[590] Ibid.
[591] Gavin Phillipson, 'Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act' (2003) 66 MLR 726 and Paul Gewirtz, 'Privacy and Speech' (2001) *Supreme Court Law Review* 139, 181–2.
[592] *Von Hannover.*
[593] See for example *Campbell*.

Conclusion

This concludes this chapter's analysis of the ECtHR's reasonable expectation of privacy test and its application to the right to be forgotten, along with its analysis of the 'balancing factors' relied on by the Strasbourg Court when assessing Article 8 claims. As elucidated above, certain factors will have more or less relevance depending on the facts of a particular claim, and it has been recommended here that if informational privacy is to be restored online, certain factors should not be used – or only in modified form by the English courts. The next chapter considers the ECtHR's balancing principles going to the weight of a competing interest in freedom of expression under Article 10 ECHR.

Chapter 4: Strasbourg and English jurisprudence concerning freedom of expression and its application to the right to be forgotten

Introduction

The previous chapter considered how best to interpret the new right to be forgotten with reference to the normative framework of Article 8 ECHR and the Strasbourg Court's wealth of privacy jurisprudence. We now turn to consider the factors going to the weight of a competing freedom of expression claim under Article 10 ECHR. As noted in chapter 1, a common theme between each area of law that this thesis examines[594] is the necessity to balance privacy and reputation rights against freedom of expression. Article 17(3)(a) contains a general freedom of expression exemption, which, if made out, negates a deletion request. As discussed in chapter 3, the GDPR and (accordingly) the Data Protection Act 2018 also encompasses a journalistic exemption.

This chapter will offer some analysis as to the balancing exercise that must be undertaken by the courts when expression and privacy rights collide, using the backdrop of the Strasbourg Court's analysis when an Article 10 claim conflicts with an Article 8 claim. Article 17 is a new right and is broadly framed, and it is important that this evaluation is undertaken to ensure that the right sits comfortably alongside the ECHR. This chapter will also include reference to English caselaw which turns on free expression or 'public interest' claims, as English courts have taken the lead from Strasbourg in ensuring that domestic law upholds Article 10 rights.[595]

A. Theoretical justifications for freedom of expression

Before this chapter analyses Strasbourg and English jurisprudence concerning free expression and applies it to Article 17(3)(a), it is important to consider theoretical justifications for free speech and its continued importance. As noted above, the right to be forgotten has generated

[594] Namely Article 17 GDPR, misuse of private information and defamation.
[595] It will be argued in chapter 5 of this thesis that at times the English courts have gone too far in this aim, and unfairly prioritised expression rights over privacy interests.

considerable debate and controversy: in particular, academics based in US institutions[596] and the UK Parliament[597] have voiced strong concerns, most often grounded in the fear that the right will have a seriously detrimental effect on speech online. It will be argued in the next section of this thesis that the three most prevalent and traditional rationales supporting expression[598] have little application to (and are not generally facilitated by) the disclosure of personal data online. In light of this, it is submitted that these concerns are largely unfounded. Therefore, this chapter as a whole will seek to argue that Article 17(3)(a)'s free expression and journalism exception:

- must not be interpreted excessively broadly in order to account for such concerns and;

- both provide a 'safety net' whereby *legitimate* speech in the public interest can, in certain situations, override a deletion request.

I. Freedom of expression is essential for the pursuit of truth

Perhaps the most prevalent rationale underpinning freedom of expression is the notion that if speech is unrestricted and all voices are heard, the truth about a given matter will be more likely to emerge.[599] This theory was proposed by John Stuart Mill,[600] and was adapted by US Supreme Court Justice Oliver Wendell Holmes. Holmes argued that this 'social

[596] See for example: Meg L Ambrose, 'It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten' (2013) 16(2) *Stanford Technology Law Review* 369, Jeffrey Rosen, 'The Right to be Forgotten' (2012) *Stanford Law Review Online* 88, Diane L Zimmerman, 'The "New" Privacy and the "Old": Is Applying the Tort Law of Privacy Like Putting High Button Shoes on the Internet?' (2012) 17 *Communications Law and Policy* 107, Paul Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 *Harvard Law Review* 1966 and W. Gregory Voss, 'One year and loads of data later, where are we? An update on the proposed European Union General Data Protection Regulation' (2013) 16(10) *Journal of Internet Law* 13.

[597] See the findings of the European Union Committee, *EU Data Protection Law: A 'Right to be Forgotten'?* (HL 2nd Report of Session 2014-2015) paper 40. The committee condemned the introduction of an erasure right, citing concerns of censorship online and difficult application in practise.

[598] That of the pursuit of truth, autonomy, self-fulfilment and facilitation of democracy.

[599] Helen Fenwick and Gavin Phillipson, *Media Freedom Under the Human Rights Act* (Oxford University Press 2006) 683-4, Kent Greenawalt, 'Free Speech Justifications' (1989) 89 *Columbia Law Review* 119, 130 and G. Edward White, 'The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America' (1996) 95(2) *Michigan Law Review* 299, 355 and Ruth Gavison, 'Too Early for a requiem: Warren and Brandeis were right on privacy vs free speech' (1992) 43(3) *South Carolina Law Review* 437, 462.

[600] Greenawalt above, 599 at 131 and John Stuart Mill, *On Liberty* (Cosimo Classics Philosophy 2009).

Darwinism'[601] helps expose the falsities advanced by large corporations or the government.[602] Additionally, if individuals' views are heard (facilitated by free speech), then people are less likely to upset established order.[603] The truth justification assumes that the pursuit of truth is inherently a good thing that benefits society at large.

This expression theory can be subject to several key criticisms. Firstly, it can be difficult for an individual to perceive accurate 'truths' when viewing selected pieces of speech or information.[604] For example, a published photograph may convey certain objective factual truths (such as where the photograph was taken) but such pictures often lack requisite context.[605] Secondly, this justification appears to make the assumption that all speech has equal value as it promotes the finding of generalised truths.[606] This aspect of the theory is problematic as it does not differentiate between data which has fundamental societal significance (discussion of which is essential for public debate resulting in the furtherance of society) and mundane pieces of personal data. The publication and subsequent discussion of the 'truths' of banal private information serves as a distraction from valuable public discussion of legitimate general interest.[607] In light of this, academics such as Greenawalt have gone so far as to suggest that *restricting* certain types of speech in particular circumstances can be helpful to finding truth[608] as this can help refocus society on issues of pivotal importance.[609]

i. The marketplace of ideas

[601] Pnina Lahav, 'Holmes and Brandeis: Libertarian and Republican Justifications for Free Speech' (1988) 4 *Journal of Law and Politics* 451, 456-8.
[602] Fenwick and Phillipson above, n 599 at 115.
[603] See Greenawalt for a discussion concerning objective and subjective truths: above, n 599 at 142.
[604] Ibid, 130. Such discrete pockets of information can come in the form of pieces of personal information on the web. Also see White above, n 599 at 133-4.
[605] See *Delete*.
[606] Gavison above, n 599 at 464. Gavison argues that most privacy-invading expression is not attempting to pursue certain truths.
[607] See Paul Wragg, 'A Freedom to Criticise? Evaluating the Public Interest in Celebrity Gossip after Mosley and Terry' (2010) 2(2) *Journal of Media Law* 295, 304-7: Wragg argues that the UK press reporting on the sexual infidelities of footballers does not advance societal interests and does not hamper serious investigative journalism.
[608] Greenawalt above, n 599 at 138 and Lahav above, n 601 at 456 and Lee C Bollinger, 'Free Speech and Intellectual Values' (1983) 92(3) *Yale Law Journal* 438, 451.
[609] The issue with this stance being 'what constitutes an issue of pivotal importance?'

The 'marketplace of ideas' is a version (or an offshoot) of the truth justification which gained prominence in the 1920s.[610] It is the controversial notion that if multiple different views are heard, whatever conclusion society will reach *should be regarded as the truth*, and was discussed by Wendell Holmes.[611] In other words, whatever emerges from the free and open marketplace of ideas should be assumed to be the truth. Greenawalt criticises this conception of speech as no checking mechanism is subsequently applied to what conclusion emerges from the marketplace.[612] However, no general test for truth has been reliably agreed on by legal academics and this criticism could be applied to the truth justification in general rather than just the marketplace of ideas. It has been questioned by Barendt whether the operation of the marketplace of ideas necessarily leads to liberal societal advancement.[613] According to Wendell Holmes' traditional conception of the marketplace, this should be a secondary concern – the majority will have their views emerge and become accepted as long as the marketplace of speech crucially remains unregulated by the government.[614]It is argued here that this speech 'metaphor' is best thought of as producing society's closet approximation to the truth,[615] rather than pure objective truth.

Finally, the truth justification for free speech does not address the fact that all voices are not heard at equal volume, due to economic and social power imbalances between speakers.[616] Therefore, the public is more likely to hear – and potentially believe – the version of the truth that large media corporations and conglomerates advocate rather than the voice of a private individual, despite the fact that the latter's speech may be more accurate. This failing of the truth justification has been amplified by the introduction of social media: high-profile speech of such corporate outlets is increasingly easy to access and, in turn, more difficult to avoid. If a news story is published online concerning a private individual, their quiet online voice in rebutting inaccurate information will often pale in comparison online especially when such a news article has been repeatedly 'shared'[617] by others and reposted to other sites.[618] To

[610] White above, n 599 at 316.
[611] Lahav above, n 601 at 456-8.
[612] Greenawalt above, n 599 at 153.
[613] Eric Barendt, *Freedom of Speech* (2nd Edn, OUP 2007).
[614] Lahav above, n 601 at 458.
[615] Much like a criminal trial in an English court, in which the jurors decide on the 'best version' of the truth after listening to submissions from both prosecution and defence counsel.
[616] Greenawalt above, n 599 at 134.
[617] 'Sharing' is the ability of an internet user to re-post an internet article that they have seen on a particular site to a different social media platform. Twitter, for example, allows a user to share a tweet on other social media or by email: see https://twitter.com/?lang=en.
[618] This would not be the same for celebrities, often who have millions of 'followers' on social media sites.

conclude, it remains unclear whether all speech being heard does lead to the public making better or more societally effective decisions as a result.[619]

II. Freedom of expression is necessary for facilitating a flourishing democracy[620]

This consequentialist speech justification is relied on extensively by the Strasbourg, English and US courts[621] as well as prominent legal academics. Meiklejohn advanced the argument that the First Amendment's value was in its ability to facilitate political process.[622] Brandeis argued that all citizens should participate in democracy[623] and in order to facilitate a functioning democratic government there must be unbridled discussion of political issues.[624] In respect of the role of the media in exercising free expression in England and Wales, Lord Justice Ward in *K v NGN* stated that:

> 'Unduly to fetter their freedom to report as editors judge to be responsible is to undermine the pre-eminence of the deserved **place of the press as a powerful pillar of democracy**.'[625]

A rationale behind this justification is the idea that the more political debate that occurs, the better educated the electorate will become about who to vote for.[626] The justification was discussed during the prominent US defamation case of *New York Times Co. v Sullivan* which introduced an 'actual malice standard'[627] that must be met if defamatory media reportage of

[619] Greenawalt above, n 599 and Lahav above, n 601 at 454-8 referencing Justice Oliver Wendell Holmes in *Abrams v United States* 250 U.S. 616 (1919).
[620] Although this is one of the most prevalent justifications for freedom of expression, it is interesting to consider that influential American academic Martin Redish argues against its continued prominence. Redish notes that despite many claiming that the First Amendment is concerned with preserving political speech, it has been shown (by the US as well as the Strasbourg courts) that many forms of none-political speech fall under the remit of its protection. He also observes that different types of political action can also facilitate democracy, rather than just political expression. See both Redish articles above, n 651.
[621] See for example *Observer and Guardian v. the United Kingdom,* App no. 13585/88 (ECHR, 26 November 1991) [59], *Axel Springer* [91] and *Von Hannover (no.2)* [110] and *K v News Group Newspapers Ltd* [2011] EWCA Civ 439 [2011] 1 WLR.
[622] See Martin H Redish, 'The Value of Free Speech' (1982) 130 *University of Pennsylvania Law Review* 591, 596.
[623] Lahav above, 601 at 460-3.
[624] White above, n 599 at 355.
[625] *K v NGN* above, n 621 at [A – emphasis added].
[626] Greenawalt above, n 599 at 145-6.
[627] In other words, ill-will or malevolent intention on the part of the author or publisher of the piece.

public figures can be considered actionable.[628] Bollinger has observed that Meiklejohn's writings had a significant impact upon the judgment in the case, the decision emphasising that freedom of the press is necessary for the public to fully engage in political process (which is ultimately beneficial to society as a whole).[629] A further rationale behind this justification is the value of free speech in its ability to hold the government to account; this deters corruption and poor governance. The justification is also related to the negative free expression theory of 'distrust of government' – that free speech stops a government from censoring radical ideas for reasons of bias.[630]

However, the amount of speech this justification can apply to is arguably narrow. Barendt argues that if its role in protecting democracy is the right's foremost justification, this can only apply to information which facilitates the general public in holding the government to account,[631] performing a 'watchdog' function (and presumably also information which helps inform individual how to vote); in other words, political information.[632] Redish concurs and observes that despite academic assertion that the First Amendment is concerned with protecting political speech, many forms of non-political speech fall under the remit of its protection.[633] Bork contests the inclusion of non-political expression (such as literature and art) under the First Amendment.[634] By way of comparison, Strasbourg 'ranks' what degree of Article 10 protection particular speech should encompass, with political speech receiving the most significant degree of protection and artistic speech having a more moderate weight.[635] It has also been postulated that different forms of political action can also help fulfil the role of democracy, rather than just political expression.[636] Baker has argued that unbridled free speech can in fact unseat established democratic order and cause ructions in society, particularly in relation to highly offensive speech.[637]

It has been stated above that this free speech justification is too narrow in its definition (as it only pertains to political speech) but it can also be argued that it is simultaneously too wide.

[628] *New York Times Co. v Sullivan* 376 U.S 254 (1964).
[629] Bollinger above, n 608.
[630] Barendt above, n 613 at 21.
[631] Ibid, 18.
[632] The 'watchdog' public interest factor is discussed in detail later in this chapter.
[633] Redish above, 'The Value of Free Speech' n 651 at 597.
[634] Ibid Redish, 597 discussing Judge Bork and see Robert H. Bork, 'Neutral Principles and some First Amendment Problems' (1971) 47(1) *Indiana Law Journal* 1.
[635] Fenwick and Phillipson above, n 599 at 689.
[636] Redish above, 'The Value of Free Speech' above, n 651 at 600.
[637] C. Edwin Baker, 'Giving the Audience What it Wants' (1997) 58(2) *Ohio State Law Journal* 311.

For example, private information relating to an important political matter is often considered by the ECtHR to be a matter of legitimate public interest. What constitutes a political matter in the eyes of the Court has been taken to have a particularly wide ambit, as was demonstrated in *Standard Verlags GmbH v Austria*,[638] a case concerning the reportage of suspected embezzlement by senior officials of a bank. The Strasbourg court held that as matters of politics and banking are often intertwined, the media coverage was protected under Article 10. Conversely, it can be stated that the view of speech as facilitating democracy can be seen as unduly restrictive: it would be contentious in Western culture for the government to censor artistic expression without a compelling reason do to so.[639]

III. Free speech is necessary for individual autonomy

The 'free speech as autonomy' justification for expression argues that individuals should have a right to decide what they see, hear and say as this is a crucial aspect of human autonomy – and free speech facilitates this (regardless of whether this will in fact have a positive effect on their life). This is 'self-governance'.[640] Objections can be levelled against the *speech as autonomy* justification. Firstly, Greenawalt argues that the notion of autonomy is expressly difficult to quantify or monitor.[641] To measure individual autonomy one must also presuppose that it is an objective factor, whereas in practice autonomy may be subjective to the person in question. For example, what someone who is resident in Saudi Arabia may consider to be a life with a high level of individual autonomy may be different to that of someone who is resident in the UK. Furthermore, the expression as autonomy justification conflicts with the theory that the right to privacy allows for individual autonomy and dignity, as was argued in chapter 2 of this thesis.[642] In essence, autonomy can be achieved *both* by effective self-governance over what one speaks, reads and writes as well as the ability to seclude oneself, allowing an individual to experiment and develop (socially or artistically) away from the watchful eyes of others.[643] This leads to a fundamental conflict of interests.[644]

---

[638] *Standard Verlags GmbH v Austria (No. 3)* App no 34702/07 (ECHR, 10 January 2012) and see Dirk Voorhoof, 'European Court of Human Rights: Standard Verlags GmbH v Austria' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2012-2/2).
[639] If for example the expression was highly offensive or in some way caused or incited harm to others.
[640] White above, n 599.
[641] Greenawalt above, n 599 at 144.
[642] Tom Gerety, 'Redefining Privacy' (1977) 12(2) *Harvard Civil Rights-Civil Liberties Law Review* 233, 265 and Thomas I Emerson, 'The right to privacy and freedom of the press' (1979) 14(2) *Harvard Civil Rights-Civil Liberties Law Review* 329, 339.
[643] Gavison above, n 599 at 464.
[644] See the 'giving accounts of different modes of living' free expression balancing-factor discussed below.

IV. Free speech as necessary for self-fulfilment/development

'Free speech as enhancing self-fulfilment' claims that free expression has a positive effect on an individual's life as access to certain speech can mean that an individual 'flourishes'.[645] The theory is that if people are exposed to information relating to various life-choices, they are increasingly likely to make informed (and therefore better) decisions in life themselves.[646] A similar criticism to that which was made above in relation to autonomy can be made of the *speech as promoting self-development* justification. Wragg has noted that justifications in favour of protecting privacy and justifications for protecting free expression (on the grounds of self-development) often conflict. When they do, many academics argue that the judiciary ought to prioritise freedom of expression.[647] Wragg defends this prioritisation of expression, and comments:

> 'Although every member of public is both a consumer and potential source of news, the **chances of the latter happening are considerably less** than the former such that it may be said that society's greater interest is in consumption and, therefore, this should be reflected in the court's treatment of the benefits-to-self argument.'[648]

Due to the rise of the digital age, the likelihood of a data subject's personal information being disseminated online (be it through a news outlet or on a social networking site) is now high, and increasing.[649] The use of social forums online is widespread and the pressure to disclose personal information online – from website operators as well as peers – is strong. As a result of this, the self-development rights of the *receivers* of information are increasing but the privacy and dignity rights of those whom the information *is about* are decreasing. It is submitted in this chapter, contrary to Wragg's argument, that this trend should be reflected by

[645] See White above, n 599 at 345, discussing the works of Thomas Emerson.
[646] Lahav above, n 601 at 459 and Greenawalt above, n 599 at 144.
[647] See chapter 2 of this thesis.
[648] Paul Wragg, 'The benefits of privacy – invading expression' (2013) 64(2) *Northern Ireland Legal Quarterly* 187, 203 [emphasis added].
[649] For example see sites Facebook: https://en-gb.facebook.com/, Snapchat: https://www.snapchat.com/, Instagram: https://www.instagram.com/?hl=en, Twitter: https://twitter.com/?lang=en (last accessed 28/11/16) all of which provide social media platforms where users interact by sharing personal information. Specialised media sites include Linkedin: https://gb.linkedin.com/ (which focuses on personal data relating to careers) and dating sites such as Match.com: https://uk.match.com/unlogged/landing/2016/06/02/hpv-belowthefold-3steps-geo-psc-bowling?klid=6740&ktid=0 which enable users to upload personal data in order to find a romantic partner (both last accessed 28/11/16).

the judiciary in privacy caselaw, in the sense that consequentialist arguments for the protection of privacy should be taken as the prevailing account when this conflicts with the narrative of expression as self-development. This argument will be developed in more detail later in this chapter, concerning the public interest in 'modes of living' balancing factor.

The core notion of speech as supporting individual self-development has been questioned by academics such as C. Edwin Baker. Baker makes three strong propositions in this regard, which can be summarised as such: i) individuals can effectively 'self-rule' without access to completely uninhibited information flow; ii) information-flow is not the only factor that enables self-rule and iii) information 'overload' can actually inhibit self-rule.[650] The first of these stipulations seems to support the argument outlined above that when consequentialist arguments in favour of privacy and self-development justifications for the importance of speech conflicts, privacy rights should prevail. Essentially, Baker argues that 'good' life decisions can be made by individuals without unfettered access to unlimited expression. For example, a person's anecdotal and personal life experience can provide a good platform upon which to make judgments. Secondly, he appears to suggest that individual self-development is comprised of more than just access to a broad degree of expression. Finally, he seems to suggest that there is such a thing as having *too much* information with which to make a decision – being overwhelmed by information can often mean that we make bad decisions.

i. Is speech a speaker right or an audience right?

A key question pertaining to the theoretical underpinnings of freedom of expression is whether it is a speaker or an audience right. Academics Baker and Redish have debated this issue at length, Baker stating speech is a speaker right and Redish that it is the right of an audience to listen.[651] Redish argues that speech is of benefit to the listener in that it furthers their pursuit of truth and self-realisation.[652] Additionally, Barendt notes that the motive (monetary or otherwise) of a speaker when imparting views or facts may have an influence over the theoretical importance of their speech – the idea being that if personal or monetary

[650] C. Edwin Baker, 'Realizing self-realization: Corporate Political Expenditures and Redish's Value of Free Speech' (1981) 130 *University of Pennsylvania Law Review* 646, 661-3.
[651] See Martin H Redish, 'The Value of Free Speech' (1982) 130 *University of Pennsylvania Law Review* 591 and Martin H Redish, 'Self-realization, Democracy and Freedom of Expression: a reply to Professor Baker' (1982) 130 *University of Pennsylvania Law Review* 678.
[652] Free speech as supporting individual autonomy will be discussed later in this chapter. See Baker above, n 650, 657.

gain influences expression, it may be of less value.[653] It is unclear why expression's speaker/audience divide has been a source of contention in legal theory. Freedom of expression must be both a speaker *and* an audience right, as if a right does not exist for a speaker to disseminate their views there will be no speech to be heard by an audience. Article 10 of the ECHR defines freedom of expression as the right to 'receive *and* impart information',[654] as does the German Basic Law (*Grundgesetz*).[655]

B. Analysis of the European Court of Human Rights' Article 10 jurisprudence

Although this thesis has argued for the need to afford greater protection to online privacy, it must be noted that in certain situations freedom of expression can, and should, prevail over privacy rights. This also applies to particular erasure claims potentially brought under Article 17. As discussed in the previous chapter, the right to be forgotten contains several exceptions a data controller can rely upon in order to negate their obligation to delete personal data, one of which relates to freedom of speech online. Article 17 states:

> '(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
>
> (a) for exercising the **right of freedom of expression**…'[656]

The importance and extent of this freedom of expression exception to the right to be forgotten remains to be seen. It suggests that, when the exemption is invoked, a balancing exercise will have to be undertaken between an erasure request and a controller who refuses to comply with the request on the grounds of freedom of expression. A related but separate exemption is contained within Article 85 of the GPDR and fleshed out in Schedule 2, Part 5 of the Data Protection Act 2018 – the journalistic exemption. In order to rely on the journalistic exemption, a much more specific test must be satisfied on the part of a controller. The previous chapter to this thesis (chapter 3, part 1) gave an explanation of the content and breadth of the journalistic exemption,[657] which will not be repeated here. However, for the sake of completeness, the 2018 Act dictates:

---

[653] Barendt above, n 613 at 24 and Baker makes a similar argument to this, pertaining to commercial speech which is only in the best interests of a company – see Baker above n 650, 655.
[654] *ECHR.*
[655] Barendt above, n 613 at 11.
[656] *GDPR*, Article 17 [emphasis added].
[657] See Chapter 3, Part 1: Article 17(3) and Article 85: exceptions to the right to be forgotten.

'*Journalistic, academic, artistic and literary purposes*

26(1)In this paragraph, "the special purposes" means one or more of the following—

(a)the purposes of journalism;

(b)academic purposes;

(c)artistic purposes;

(d)literary purposes.

(2)Sub-paragraph (3) applies to the processing of personal data carried out for the special purposes if—

(a)the processing is being carried out with a **view to the publication** by a person of journalistic, academic, artistic or literary material, and

(b)the controller **reasonably believes that the publication of the material would be in the public interest.**

(3)The listed GDPR provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes.

(4)In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.

(5)In determining whether it is reasonable to believe that publication would be in the public interest, the **controller must have regard to any of the codes of practice or guidelines** listed in sub-paragraph (6) that is relevant to the publication in question.

(6)The codes of practice and guidelines are—

(a)BBC Editorial Guidelines;

(b)Ofcom Broadcasting Code;

(c)Editors' Code of Practice'.[658]

[658] Data Protection Act 2018, Schedule 2, Part 5, paragraph 26 (1)-(6) [emphasis added].

As stated in chapter 3 Part 1 the above 'test' for this exemption can be summarised as such:

I. the personal data must be processed with the **intention to publish** the information as journalistic material;

II. a controller's **reasonable belief** that doing so is in the **public interest**;

III. a controller's reasonable belief that applying the relevant GDPR principle would **hinder this journalistic motive**;

IV. A controller must be **aware of relevant privacy codes and follow them explicitly**.

This chapter will consider expression arguments that could be run by defendant controllers in order to rely on either Article 17(3)(a) or Article 85's journalism exemption in order to negate an erasure request. It is crucial that an appropriate balance is struck between ensuring robust data protection and the maintenance of important and valuable speech online. As has just been evaluated, the right of freedom of expression has enormous historical and theoretical importance, as well as substantive importance for the individual and society. This chapter will consider several balancing principles that the ECtHR and the English courts employ when assessing the strength of an interest in expression under Article 10 against a competing claim to privacy. It will apply these principles to potential erasure requests under the right to be forgotten and the interpretation of its scope.

I. What is 'publication in the public interest'?

The 'public interest' is perhaps the most frequently cited balancing principle that Strasbourg employs when evaluating the strength of an Article 10 claim, and in the eyes of the English courts is a 'decisive factor'[659] – as noted above, *intended publication in the public interest* is a requirement to rely on the Data Protection Act 2018's journalism exemption. Indeed, the notion of publication in the public interest dominates expression jurisprudence in defence to a

[659] Wragg above, n 648 at 189.

competing privacy claim. Despite its prevalence in free expression jurisprudence, the notion of public interest is notoriously difficult to define, Wragg commenting that it is a 'continuum'.[660] Trends of judicial reasoning have emerged both in Strasbourg and the English courts with regards to broad and increasingly narrow conceptions of the public interest in various cases at different times. The ECtHR has adopted *both* expansive and constrictive approaches to what it deems a matter of public interest and, as a result, the Strabourg Court's precedent on this matter can appear contradictory. In *Sæther v. Norway* the court stated that the life of a popular performing artist would be a matter of public interest:

> 'The definition of what constitutes a subject of general interest will depend on the circumstances of the case. The Court nevertheless considers it useful to point out that it has recognised the existence of such an interest not only where the publication concerned **political issues or crimes**, but also where it concerned **sporting issues or performing artists**'[661]

Yet in *Von Hannover v Germany (No.2)* the court adopted the opposing view in relation to famous singers:

> '…the rumoured marital difficulties of the **President of a country** or the **financial difficulties of a famous singer were not deemed to be matters of general interest**…'[662]

In *Von Hannover v Germany* the Strasbourg court delivered a well–reasoned judgment in finding that there was not a legitimate or overriding public interest in relation to pictures of Princess Caroline of Monaco, depicting the Princess going about her daily life.[663] The court stated that this was due to the fact that Caroline was not engaged in any official function while the photographs had been taken, and the images relatedly solely to her personal life.[664] However, in *Von Hannover v Germany (no.2)* the ECtHR adopted a position less favourable to Caroline's privacy rights. Here the court held that Princess Caroline's Article 8 interests

[660] Ibid, 189.
[661] *Lillo-Stenberg* [36 – emphasis added].
[662] *Von Hannover (No.2)* [109 – emphasis added] also see Gavin Phillipson, 'Press freedom, the public interest and privacy' in Andrew Kenyon (Ed) *Comparative Defamation and Privacy Law* (CUP 2016) 154.
[663] *Von Hannover*.
[664] *Von Hannover* [76] and Alastair R Mowbray, *Cases and Materials on the European Convention on Human Rights* (Oxford University Press 2007) 582.

were trumped by a public interest concerning a magazine article detailing that her father, Prince Rainier, had been ill. The Court held that since the Prince was a member of a royal family he thereby garnered much attention and importance in the eyes of the public, his ill health a prominent 'event of contemporary society.'[665]Therefore, certain photographs relating to this matter could be published.[666] The court however found that other photographs of the Princesses' family within the article, unrelated to this matter, did not constitute a matter of legitimate public interest as they were for 'entertainment purposes alone' and should be suppressed.[667] The position of the court in this regard has been rightly criticised, with Phillipson arguing that there was a tenuous the link between the public interest value within magazine article and the selected pictures that the court deemed protected by Article 10.[668]

In *Von Hannover v Germany (no.3),* the Strasbourg court appeared to further distance itself from its strong protection of Article 8 rights in *Von Hannover v Germany* and adopted an unduly broad approach with regards to what constitutes a matter of legitimate public interest. Here the court found that publication of an article discussing the holiday home of Princess Caroline and her husband (alongside pictures of the family) was protected under Article 10, despite the fact the article contained seemingly banal information relating to the price and furnishings of the property.[669] It could be argued that although such a piece may generate mild curiosity within some members of the public, it is more difficult to envisage how such an article could constitute a matter of *legitimate* or important public interest. Phillipson argues that a shift has occurred within the ECtHR towards widening what private information it perceives to be in the public interest to disclose, evident from the court's incremental change in position between *Von Hannover v Germany (nos. 1, 2 and 3).*[670] It is submitted here that this Strasbourg trend towards an expansive definition of the public interest will not work in the favour of enforcing a comprehensive right to be forgotten, if this is adopted by the English or European courts. If the ambit of Article 17(3)(a)'s expression exception is construed widely this would rid the erasure right of its power to reinstate privacy and forgetting, as deletion requests may often be trumped by an (albeit marginal) aspect public interest in the personal information concerned. Interestingly, there is some evidence to

[665] *Von Hannover (no.2)* [118].
[666] Ibid.
[667] Ibid [118].
[668] Phillipson above, n 662 at 153.
[669] *Von Hannover (No.3)* and Alexia Bedat, 'Case Law, Strasbourg; Von Hannover v Germany (no.3) Glossing Over Privacy' (*Inforrm*, 13 October 2013) available at; https://inforrm.wordpress.com/2013/10/13/case-law-strasbourg-von-hannover-v-germany-no-3-glossing-over-privacy-alexia-bedat/ (last accessed 25/5/16).
[670] Phillipson above, n 662 at 152.

suggest that Strasbourg jurisprudence may be altering *again* in order to take into account the changing nature of privacy rights in the internet age. In May 2016 the judgment of *Fürst-Pfeifer v Austria*[671] was issued. The case concerned the Article 8 rights of a claimant regarding an article data distributed about them (both on paper and online). Dissenting Judges Wojtyczek and Kūris observed that:

> 'there must be growing awareness of the increasingly pressing need to ensure more effective protection for personality rights, in particular privacy rights, *vis – à – vis* a progressively all – powerful media, acting under the aegis of "public interest".'[672]

Both judges went on to note the potential of the modern media to 'mushroom its intrusions into individuals' privacy'[673] and European reliance on the right to be forgotten to uphold privacy rights.[674] Whether this heralds a changing trend in ECtHR privacy precedent remains unclear, particularly in light of the fact that Judges Wojtyczek and Kūris' opinions were in the minority, the majority of the court in the case deciding to uphold Article 10 interests.[675]

The evidence of an unduly broad approach to what constitutes the public interest is perhaps more prevalent in English than Strasbourg jurisprudence. For example, within the judgment of *Goodwin v News Group Newspapers* the English courts declared it was in the public interest to know that the married CEO of a bank had embarked upon a romantic affair with a colleague, despite the fact that he was not a well-known public figure and the nature of the information was inherently intimate.[676] Wragg notes that it appears that English courts adopt the position that if there is *some aspect* of a public interest in the personal data at issue this automatically overrides a competing privacy claim.[677] Therefore the courts' assessment stops at this juncture, rather than going on to further consider the *weight* of the public interest

---

[671] *Fürst-Pfeifer v Austria*, App. nos. 33677/10 and 52340/10 (ECHR, 17 May 2016) and Stijn Smet, Fürst – Pfeifer v Austria: "A one-sided, unbalanced and fundamentally unjust argument" (Strasbourg Observer, 16 June 2016) accessible at: https://strasbourgobservers.com/2016/06/16/furst-pfeifer-v-austria-a-one-sided-unbalanced-and-fundamentally-unjust-judgment/.
[672] Ibid.
[673] Ibid.
[674] Ibid.
[675] Ibid.
[676] The information rendering likely ill – effects to the reputation and emotional wellbeing of the man concerned upon informational release. See *Goodwin v News Group Newspapers (no.3)* [2011] EWHC 1437 (QB) and Wragg above, n 648 at 191. Also see the previous section of this chapter discussing the relevance to competing privacy/speech interests of the intimacy of data.
[677] Wragg above, n 648 at 198 and see for example *Ferdinand* and *Hutcheson (previously "KGM") v News Group Newspapers Ltd* [2011] EWCA Civ 808.

involved, such as its contribution to an important debate[678] and then balancing this against the strength of the privacy claim. He aptly observes that the English courts are adopting a skewed interpretation of ECtHR jurisprudence as to what constitutes the public interest, by failing to conduct an adequate balancing exercise between privacy and expression rights.[679] It is submitted here that this patent lack of balancing between rights serves as an example of *what should not continue* when the courts' interpret Article 17 and its freedom of expression exception and journalism exemption. The purpose of an introduction to a deletion right in Europe is to rebalance a lack of privacy rights for personal data online.[680] If any degree of public interest means that expression automatically prevails over an erasure request in this manner the efficacy of the right to be forgotten would be substantially reduced.[681]

The above section of this chapter has attempted to give an overview of some of the broad and narrow interpretations of what constitutes the 'public interest' that the English and Strasbourg courts have expounded in the past. What constitutes the public interest is a fraught legal area, and in order to determine whether a publication is legitimately in the public interest, several 'balancing factors' can be extracted from the caselaw as a guide. The next part of this chapter will analyse various sub-factors of the public interest; in other words, arguments which indicate when dissemination of private information may further social goals. This section will now go on to discuss the varying definitions of the public interest by Strasbourg as well as the English judiciary and how they can be used to interpret Article 17's (3)(a) exception and journalism exemption.

i. Accountability of individuals in public office: the press as a watchdog

Perhaps one of the most long-standing and well-known sub-categories of information in the public interest is private data exposing wrongdoing or incompetence in public office, the

[678] Ibid Wragg, 198.
[679] Ibid.
[680] See *Delete*, Daniel Solove, 'Speech, Privacy and Reputation on the Internet' in Saul Levmore & Martha Nussbaum's (Eds), *The Offensive Internet* (Harvard University Press 2010) and Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (22 January 2012) available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (last accessed 18/6/15).
[681] The balancing exercise conducted by the English courts in its MPI caselaw will be discussed in detail in the next chapter of this thesis.

publication of which holds those in power to account, with the media acting as a 'watchdog'.[682] In other words, free speech works to trump privacy-related interests in order to uncover corrupt or incompetent officials.[683] This sub-factor relies on two central justifications. Firstly, as Baker observes, it operates as a deterrent:

> 'This function involves both the media's power to expose governmental misdeeds and its ability to deter those misdeeds by increasing the likelihood of exposure.'[684]

Secondly, the press acting as a watchdog can promote the best use of public money. If a person in public office is not performing their role in an appropriate manner[685] resources can be reallocated accordingly, the officer's employment terminated and reform addressed.[686] The watchdog function therefore generates two different aspects of societal good. The idea of the press as a watchdog finds authority in both ECtHR and English jurisprudence.[687] An example of this sub-factor in operation is present in the case of *Krone Verlag GmbH & Co. KG v. Austria*, where the Strasbourg court afforded Article 10 protection to a journalistic piece exposing a member of the European Parliament who had unjustly enriched himself by claiming a teacher's salary[688] – the court noting that this was an obvious matter of public interest.[689]

a. The press as a watchdog's application to the interpretation of Article 17(3)(a) and the journalistic exemption

In order to understand the extent of this factor and its application to Article 17, it is important to clarify whom the courts consider to be an individual performing an official function. The distinction between a celebrity and someone who performs an official function appears to be that the former is someone well-known to the general population and the latter is a person whom exercises authority on behalf of the state. The Strasbourg Court has held that Princess Caroline held no position of responsibility for the state of Monaco and she therefore did not

[682] *Von Hannover v Germany (no.2)* [102].
[683] Diane Zimmerman, 'Requiem for a Heavyweight: A farewell to Warren and Brandeis's privacy tort' (1983) 68(2) *Cornell Law Review* 291, 326.
[684] Baker above, n 637 at 355.
[685] Perhaps due to mishandling funds or through reasons of bias.
[686] Baker above, n 637 at 355.
[687] For example, *Von Hannover (no.2)* and *K v NGN* above, n 621.
[688] Which he was not entitled to while working full-time for the European Union.
[689] *Krone Verlag GmbH & Co. KG v. Austria* App no 34315/96 (ECHR, 26 February 2000) [36].

exercise public office.[690] Conversely, in a broader reading of the watchdog principle within the English case of *Trimingham*, Mr Justice Tugendhat found that the claimant was not a 'purely private person' because she:

- **worked** for someone who wished to be **democratically elected**;
- *that* person was asking voters to trust them;
- she was a '**spin doctor**.'[691]

The English courts extend this notion of authority to not only those who hold office, but those who are running for office and their aides.[692] This reading of what constitutes an authority figure was also demonstrated in the 2018 case of *NT1 and NT2*,[693] the first 'right to be forgotten' delisting-request case heard in the English courts following *Google Spain*.[694] In the case, Lord Justice Warby noted that Article 29 Working Party suggested a broad reading of who could be considered a 'public figure' in their guidance – as 'individuals who, due to their functions/commitments, have a degree of media exposure.'[695] The judge held that because NT1 was a businessman, he would therefore be seen as a public figure – and that he was also known to the public because of his fall from grace (his criminal conviction). Utilising this factor, Lord Justice Warby tipped the balance in favour of personal data about the claimant continuing to be available on Google searches, as the purpose behind this balancing factor is that it acts as a *disincentive for improper conduct*.[696] The judge reasoned this *despite the fact* that NT1 did not hold a public office – rather, he was involved in private business ventures.[697]

The ECtHR deems that there are different acceptable levels of personal scrutiny depending upon the type of office:

'…**civil servants acting in an official capacity are, like politicians, subject to**

[690] *Von Hannover* [62].
[691] See *Carina Trimingham v Associated Newspapers Limited* [2012] EWHC 1296 (QB) and Sophie Mathiesson and Eric Barendt, '*Carina Trimingham v Associated Newspapers*: A right to ridicule?' (2012) 4(2) *Journal of Media Law* 309, 313.
[692] Ibid.
[693] *NT1 and NT2*.
[694] *Google Spain*.
[695] *NT1 and NT2* [137-8].
[696] *NT1 and NT2* [137].
[697] Who did float shares on the stock exchange – *NT1 and NT2*.

> **wider limits of acceptable criticism than private individuals**. However, it cannot be said that civil servants knowingly lay themselves open to close scrutiny of their every word and deed **to the extent politicians do**.'[698]

Hughes has noted that caselaw of the ECtHR has deemed a public figure to include 'businessmen, journalists and lawyers, well-known academics, as well as other persons who have a "position in society" or have "entered the public scene" rendering the scope of its application difficult to predict' – indeed, this is a seemingly broad list.[699]

The idea of the 'press as a watchdog' could become relevant to an erasure claim under Article 17 if the data subject holds public office or is in a position of comparable influence in the private sector.[700] It is submitted here that the 'press as a watchdog' function of the public interest should only be applied to those who have genuine positions of importance or significance to society at large although they do not have to be exclusively elected officials – as distinctions between who or who is not a public figure are not 'binary'[701] or clear cut. However, to avoid a 'slippery slope', it is argued here that in order to hold that someone is a public figure (and therefore freedom of expression with regards to their information is more likely to win out in a privacy-expression balancing exercise) there should be a tangible link between the private behaviour disclosed and a legitimate impact on the public; otherwise, the public interest factor could cover an ever-increasing amount of individuals. If this were to happen, the factor would be used as a mere tool to extend the public interest argument, even in the event that there was little meaningful in the activity that the press were 'watching over'. By way of example, English Court's extension of 'public office' in *Trimingham* to those who *work for someone* who is attempting to become democratically elected is illogical and over-inclusive.[702] If the English Court's reasoning in the case was applied to the right to be forgotten's (3)(a) exception or journalism exemption, any person who has a professional (or perhaps even personal) relationship with an individual who is campaigning to hold an official function may not be entitled to secure the removal of their information.[703] It is clear

[698] *Pedersen and Baadsgaard v Denmark* App no 49017/99 (ECHR, 17 December 2004) [emphasis added].
[699] Kirsty Hughes, 'The Public Figure Doctrine and the Right to Privacy' (2019) 78(1) *Cambridge Law Journal* 70, 73.
[700] For example, this could include Rupert Murdoch – although the press mogul is not a democratically elected official, he doubtless is an influential public figure due to his control over major newspapers and corporations.
[701] Hughes above n 699 at 77-789.
[702] Wragg above, n 648 at 200.
[703] In the abovementioned case of *Trimingham*, the claimant had both a personal and professional relationship with a person running for public office.

to see that this catchment area is unduly broad in scope, as it reduces privacy rights by virtue of association.

This factor could have relevance to Article 17(3)(a) or the journalism exemption insofar as the data concerned relates to a person's suitability for public office or their behaviour while performing that role. However, it is important to consider that individuals (including the electorate) may have varying opinions as to what constitutes personal information *having a bearing upon a person's fitness for public office*. For example, a particularly traditional or religious voter might feel that the fact a politician is homosexual would be relevant to their suitability for being an MP. Therefore, it is submitted that there must be a *direct link* between the official function of a public office (or private-sector role of equivalent importance) and the personal information in question. Such information may expose particular tensions between the personal life of the person concerned and the performance of their job. This position is somewhat supported by the ECtHR in the cases of *Von Hannover v Germany (no.2)* and *Standard Verlags*.[704] The Strasbourg court suggested that if private information has a bearing on the ability of the person in question to perform their official function, then it ought to be disclosed.[705] As Matthieson and Barendt note, in order to justify such a personal intrusion there must be a *direct connection* between that aspect of an individual's private life and the performance of their public function or political role.[706] The Strasbourg Court elaborated upon this issue in *Verlags*, suggesting that a person's sexual life would seldom be considered relevant to their ability to do their job, other than in specific circumstances.[707] Such a circumstance may arise if the individual was an MP seeking to remove information about a romantic relationship that created a conflict of interests within her parliamentary role.[708] This approach echoes the US courts' distinction between 'general' and 'limited' public figures. Under the assessment of the American courts, the publication of private information relating to a limited public figure is only permissible if it relates to aspects of their private lives associated with their reason for fame or public office.[709] In this capacity, the watchdog principle has a certain degree of relevance towards data subjects in public office pursuing erasure requests.

[704] *Von Hannover (no.2)* [110] and *Standard Verlags GmbH v Austria (no.2)* App no 21277/05 (ECHR, 4 June 2009).
[705] Ibid *Standard Verlags*, [51].
[706] Mathiesson and Barendt above, n 691 at 313.
[707] *Standard Verlags* above, n 704 [48 and 51] and *Von Hannover (no.2)* [110].
[708] For further reading see John Elwood, 'Outing, Privacy and the First Amendment' (1992) 102 *Yale Law Journal* 747.
[709] Although presumably who is a 'limited public figure' could be contested. See *Sullivan* above, n 628.

ii. The public interest in private information as giving an account of a particular mode of living

This factor argues that a substantial flow of personal information is valuable as it gives accounts of particular modes of living, allowing an observer to 'personalise' a range of topics. Zimmerman summarises the notion by stating: 'all information is potentially useful in some way to the public in forming attitudes and values. Thus every communication is arguably privileged.'[710] Founder of the US privacy torts, Prosser, believed that there is a correlative increase between the amount of personal information an individual has access to and the productivity in life choices that they themselves are able make.[711] The justification for this is that if a person is exposed to alternative styles of living their judgement improves with regards to decisions in their own personal lives – as they have a greater wealth of knowledge and experience to draw upon.[712] Raz clarifies this factor's theoretical basis:

- '[it serves] …to **familiarize** the public at large with ways of life common in certain segments of the public…
- …to reassure those whose ways of life are being portrayed that they are **not alone**, that their problems are common problems, their experiences known to others.
- [it serves] as **validation** of the relevant ways of life. They give them the stamp of public acceptability.'[713]

The central downfall of this argument is that it is over-inclusive.[714] The argument fails to draw any limitations upon the amount or type of personal information disclosed about an individual in order to give a lifestyle account. As Elwood observes, it has traditionally been argued by 'pro-outing'[715] activists that exposing a person as gay serves as an important message to society – the message being that alternative sexualities other than heterosexuality

[710] Zimmerman above, n 683 and also see Eugene Volokh, 'Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People Speaking About You' (2000) 52 *Stanford Law Review* 1049.
[711] Ibid Zimmerman and Eric Posner, 'The Right of Privacy' (1978) 12 *Georgia Law Review* 393 (Zimmerman quotes Posner in her article).
[712] Ibid Zimmerman at 354 and Posner.
[713] Joseph Raz, 'Free Expression and Personal Identification' (1991) 11 *Oxford Journal of Legal Studies* 303, 309–11 [emphasis added] and also see Phillipson n 662 as well as Wragg above, n 648.
[714] Ibid Raz, 313 and Phillipson 141.
[715] In other words, publicly revealing that a person is homosexual.

exist.[716] However, this argument fails to take into account the consent of the person in question to having their sexuality broadcasted publicly. It is important to note that throughout the 1960s to the 1980s many people suffered as a result of a trend in non-consensual 'outing', particularly financially through loss of work and personally, through estrangement by their friends and families.[717] Indeed, the 'account of modes of living' factor's central failure is its lack of *meaningful* consideration of the needs, desires or harms done to an individual on publication of private facts – and the assumption that the benefits of revealing private information are often more important for society as large. It does not respect the personal autonomy and dignity of a data subject, manifested in a decision to make only certain details about themselves public and the important need for seclusion.[718]

A further justification for this balancing factor is that exposure to different lifestyle choices help facilitate change to cultural traditions and the acceptance of new forms of living.[719] Yet this does not take into account the opportunity for an individual's self-reflection that privacy allows, or the ability for a person to be able to experiment with different lifestyles away from the public eye, directly leading to different philosophies on how to behave.[720] Zimmerman makes a vague argument to support this balancing factor, stating that in order for society to function it is necessary for citizens to know information about one another.[721] Zimmerman does not detail the quantity or content of information that she encompasses in her statement. This is indeed true to an extent – it is necessary for an individual to disclose *certain* pieces of personal information to *particular* individuals in their daily lives. For example, a person would tell their milkman whether they prefer to drink whole or skimmed milk and would likely disclose to their best friend if they were recently bereaved.[722] However, in such situations an individual has informational control over *who* they tell, and *what* they tell them.[723] Conversely, if a person's private details are published in a newspaper or disclosed online by a third party then this is often absent of the individual's genuine consent.

[716] John Elwood, 'Outing, Privacy and the First Amendment' (1992) 102 *Yale Law Journal* 747, 772.
[717] Ibid.
[718] See Chapter 2 of this thesis, under the subheading of 'the protection of an individual's dignity'.
[719] Raz above, n 713 at 312.
[720] See Chapter 2 of this thesis, 'Encouraging personal creativity and growth' as well as Jeffrey Rosen, 'Why Privacy Matters' (2000) 24(4) *The Wilson Quarterly* 32, 38 and Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89(3) *The Yale Law Journal* 421.
[721] Zimmerman above, n 683 at 326.
[722] Not least because a milkman would need to know what type of milk to deliver and a friend need to know about a bereavement to offer emotional support.
[723] See 'control-based definitions of privacy' in chapter 2.

Zimmerman does not address that most personal information is relatively banal with no bearing upon the 'fabric' of society.[724]

a. Giving an account of a particular mode of living's application to the interpretation of Article 17(3)(a) and the journalism exemption

It is submitted here that little heed should be given to this factor by the domestic courts when seeking to establish the limits of Article 17's freedom of expression exception or journalism exemption. The central justification that this balancing factor invokes[725] is a weak one. To criticise the factor on its own terms, there are many different ways that the public (or an online audience) can learn about different modes of living rather than through reading private exposés online.[726] Many forms of media contain information about different lifestyle decisions and habits of living, including (but not limited to) books, plays, poems and historical events. There are also many individuals who choose to continuously and voluntarily disclose facts about their personal lives. A contemporary example of the latter is American former Olympian and reality television star Caitlyn Jenner who underwent a gender transition in 2015 while filming a documentary to chronicle her new life.[727] Brimblecombe and Phillipson have also noted that there has been a 'boom' in personal diary blogs online, publicly accessible, often with anonymised authors.[728]

Aside from critique of the argument on its principles, it can also be said that the factor supports draconian invasions of privacy. Application of this factor to the interpretation of the right to erasure would yield concerning results: it could be argued that *any* personal information online should remain accessible in order to make internet users feel secure in their own lifestyles or to improve their ability to make successful decisions regarding their habits of living. It is argued that this factor represents an example of how the notion of 'publication in the public interest' has been stretched.[729] It uses the premise that *even intimate*

[724] Social networking sites are increasing in popularity, yet much of the personal information on them is mundane or only holds interest for a select quantity of individuals.
[725]The importance of the publication of another's private information to inform others about differing lifestyle choices.
[726] Phillipson above, n 662 at 141 and Raz above, n 713 at 310–11.
[727] The documentary is entitled 'I am Cait' and is broadcast on E! television network. It begun in July 2015 and as of 2/10/16 has just completed its second series.
[728] *Brimblecombe and Phillipson*, 19.
[729] See Geoffrey Gomery, 'Whose autonomy matters? Reconciling the competing claims of privacy and freedom of expression' (2007) 27(3) *Legal Studies* 404, 414 and Paul Gewirtz, 'Privacy and Speech' (2001) *The Supreme Court Review* 139, 154.

private information should be shared, regardless of the unduly harmful negative impact on a data subject, simply because it gives a lifestyle 'account'. This manifestly incorrect interpretation of the public interest conflicts with ECtHR precedent, in the sense that this interpretation of the 'public interest' seemingly does not consider reputational interests of data subjects. The Strasbourg Court has noted that negative effects on a party's reputation would give rise to a heightened claim to privacy and such interests must be balanced against the right of the public to be informed of an issue in contemporary society.[730] In *Hachette Filipacchi Associés v. France*, the ECtHR sought to emphasise that the impact on an individual and their family of having private information distributed is a crucial consideration when balancing Article 10 against an Article 8 claim.[731] Furthermore, in the cases of *Lindon, Otchakovsky-Laurens* and *Bladet Tromsø* the court stated that the reputation of others is a legitimate justification in restricting expression under Article 10(2).[732]

iii. The role model argument and correcting false impressions

These are two frequently referenced balancing factors in English privacy caselaw and at Strasbourg,[733] which, if present in an action, often tip the scale in favour of disclosure of personal information. Firstly, the 'role model' argument contends that if a person is a figure of leadership or some degree of importance in society, personal information regarding their transgressions ought to be published in the public interest. Secondly, the 'correcting false impressions' factor states that if an individual has been seeking to project a misleading image to society, personal information which reveals this should be published in the public interest. It could be said that these factors both relate to the *pursuit of truth* freedom of expression-justification in 'bringing someone down from their pedestal' and exposing misleading depictions of a person to society. These factors and their application to Article 17 will now be dealt with in turn.

a. Who is a 'role model'?

[730] *Lindon, Otchakovsky-Laurens and July v France* App nos. 21279/02 and 36448/02 (ECHR, 22 October 2007) [44] hereafter '*Lindon*' and *Bladet Tromsø and Stensaas v. Norway* App no. 21980/93 (ECHR, 20 May 1999) [67 and 73] hereafter '*Bladet*'.
[731] *Hachette Filipacchi Associés v. France*, App no. 71111/01 (ECHR, 14 June 2007) [49].
[732] *Lindon* [44] and *Bladet* [67 and 73].
[733] See for example *Axel Springer.*

A broad interpretation of who constitutes a 'role model' has been prevalent within the jurisprudence of the English courts. Indeed, Phillipson observes that role model status has been applied to individuals who perform no public function and have been 'thrust into the limelight through tragedy [or mishap]'.[734] This is demonstrated in the case of *A v B*, where Lord Woolf sought to emphasise that a legitimate interest arises pertaining to someone in the public eye, regardless of whether they have *voluntarily* placed themselves there or otherwise.[735] Another example of the vast reach of the role model argument was shown in *Spelman v Express Newspapers* which justified the disclosure that a son of a MP who played minor–league rugby was taking drugs to enhance his performance.[736] The role model argument is also unwaveringly applied to professional sportsmen and women by the English judiciary,[737] regardless of whether or not the sportsperson has made any effort to garner celebrity status or present themselves as someone to look up to.

b. Criticisms of the role model balancing factor

The justification of the role model balancing factor appears to stem from the idea that a person in the limelight's behaviour has influence over their fans. This theory was given prominence by the ECtHR in *Axel Springer*, where the Court held that a popular German television actor's fans had a public interest in knowing that he had been arrested on drug charges.[738] The English courts concurred with this standpoint in *Ferdinand*, where it was stated that the moral wrong of professional footballer Rio Ferdinand being unfaithful to his partner ought to be disclosed to fans who looked up to him and his lifestyle.[739] The role model balancing factor can be criticised in three ways. Firstly, there is not a clear link between it and information in the public interest.[740] Despite the premise of this factor stating that information concerning a role model's misdemeanours should be published to their fans, little consideration appears to have been given to the effect of this information on the fans in question. Professional athletes accrue varied followings including many young admirers, who

[734] Phillipson above, n 662 at 154, bracketed text added.
[735] See *Ferdinand v MGN* [2011] EWHC 2454 (QB) hereafter '*Ferdinand*' [87], which quotes this section of Lord Woolf A v B while discussing the role model argument and the original judgment: *A v B Plc and Another* [2002] EWCA Civ 337.
[736] *Jonathan Spelman (by his Litigation Friends Mark Spelman and Caroline Spelman) v Express Newspapers* [2012] EWHC 355 (QB) [22].
[737] *Ferdinand* [87] and also see *Terry and persons unknown* [2010] EWHC 119 (QB), hereafter '*Terry*'.
[738] *Axel Springer*.
[739] *Ferdinand* [87]
[740] Phillipson above, n 662 at 155.

upon hearing such information may (rather than be dissuaded against similar behaviour themselves)[741] think such behaviour was legitimised as their favourite sporting personality has engaged in it. Disclosure of such data may therefore work actively *against* the public interest in its indirect encouragement of immoral or dangerous behaviour.[742]Secondly, in a more general criticism of this factor, it can be argued that a fan's modification of their behaviour (on receipt of this information) is hardly a matter of important or societal interest, and little explanation is given by the English courts or the ECtHR as to why such emphasis is placed on this occurrence.[743] It is difficult to see how the subjectively moral wrong of Rio Ferdinand's affair has an impact upon the 'fabric of society' in terms of the public interest.[744] Finally, Fenwick and Phillipson have gone as far as to discredit the underlying relevance of this balancing factor as a whole, by questioning whether there is any credible evidence that a role model's immoral conduct will in fact meaningfully influence the public, in either a positive or negative manner.[745]

c. Rationale behind the 'correcting false impressions' factor

The legal rationale behind the 'correcting false impressions' factor is that it is justifiable to disclose personal data about an individual in order to correct an unrealistic or misleading impression that they have chosen to establish.[746] A modern example of this factor in practice is within the case of *NT1 and NT2*.[747] In the case, the first claimant, NT1, had requested delisting to several links describing his prior criminality. It also emerged that he had hired a reputation 'clean-up' agency in order to manage his image online – which involved the firm posting accolades about his business integrity online, despite the fact he had been convicted for a dishonesty offence in relation to his business activities and served jail time.[748] Lord Justice Warby noted:

[741] Which presumably is the intended outcome of disclosing such information in the public interest: see Wragg above, n 648 at 196.
[742] Phillipson above, n 662 at 155-156. 'Immoral' behavior could arguably include adultery, whereas 'dangerous' behavior could include taking recreational drugs.
[743] Ibid Phillipson, 157 and Wragg above, n 648 at 196.
[744] Ibid Wragg, 195.
[745] Fenwick and Phillipson above, n 599.
[746] *Campbell*: see arguments made in favour of the publication of pictures of Naomi Campbell outside a drug rehabilitation meeting centre, citing that this was justified as she had sought to present herself as a model who did not take illegal drugs in order to manage her weight or lifestyle.
[747] *NT1 and NT2*.
[748] *NT1 and NT2* [130].

> 'His criminal past was also relevant…to anybody who read or might read the blog and social media postings which the claimant, via Cleanup, put out about himself. Those postings were false or misleading, and in my judgment unjustifiably so.'[749]

Lord Justice Warby found against the claimant in the case. The judge also deemed it relevant that NT1 had engaged in business ventures *since* his conviction,[750] and that a potential client could seek information about him online to be greeted with a false barrage of overwhelmingly positive data. This case has a unique set of circumstances; there is an obvious public interest in NT1's prior criminality being known as he was seeking to hold himself out to the general market as an unblemished businessman later in time. NT1 turned on its own peculiar set of facts, however, the English courts have failed to expressly articulate in *general terms* why that it matters if a misleading impression is held. As stated earlier, it seems to hinge upon the truth justification for freedom of expression; indeed, the submissions of counsel in *Ferdinand* aptly demonstrate this factor's role in the pursuit of truth:

> 'The Defendant argued that the Claimant had embarked on a wider campaign since 2006 to project a more responsible and positive image than the reputation which he had had in the past. His charitable and business activities were part of this. Here, too, the Defendant argued, there was a public interest in **demonstrating that this was misleading** because his relationship with Ms Storey [his lover] had continued long after the time when he was supposed to have changed.'[751]

This truth–seeking rationale can also be found in judgments of the ECtHR. In *Plon (Societe) v France* defendant counsel sought to argue that the public had an interest in knowing the truth behind the lies they had been told concerning the health of the French Prime Minister.[752] Wragg notes that when interpreted widely, this may encompass not only behaviour that contradicts something an individual has previously said but behaviour which is against commonly accepted societal morality at the time; making this balancing factor similar in nature to the role model argument.[753]

---

[749] *NT1 and NT2* [168].
[750] *NT1 and NT2* [121].
[751] *Ferdinand* [74 – emphasis added].
[752] *Plon (Societe) v France* App no 58148/00 (ECHR, 18 May 2004) [40].
[753] Paul Wragg, 'A Freedom to Criticise? Evaluating the Public Interest in Celebrity Gossip after Mosley and Terry' (2010) 2(2) *Journal of Media Law* 295, 307.

d. Criticisms of the correcting false impressions balancing factor

Criticisms of this public interest factor largely relate to its scope; indeed, it could be invoked to bolster publication of any material which may give the general public a more accurate picture of the person under scrutiny. This claim is cemented by this factor's relationship to the truth justification for free speech. However, it is submitted that this approach should be avoided with regards to not only the interpretation of Article 17, but also to speech-privacy balancing more generally. The false impressions factor lacks an appreciation of why and for what purpose individuals may choose not to disclose certain details. No justification is given for why exposing (often mundane) private facts about individuals and proving them dishonest is in the public interest. Elwood powerfully argues that it is only right to disclose personal data – regardless of whether it serves to rectify a false impression – if an important matter of societal importance is involved, as this finds a balance between the harm done to personal autonomy and dignity when private information is revealed and the public's desire to know the truth.[754]

e. Application of both to Article 17(3)(a) and the journalism exemption

In relation to the right to be forgotten, it is unlikely that a role model argument will apply unless the person in question is well known. It is argued that the English courts should strive to abandon the role model factor when interpreting Article 17 because its theoretical rationale lacks both logic and evidence. As discussed above, due attention has not been given to a circumstance where a young fan is made aware of potentially criminal or otherwise risky behaviour of their idol, and due to their age or lack of experience, seeks to emulate them. The 'press as a watchdog' factor performs the task of holding those in public office accountable for their misdeeds and it is difficult to see what further information of legitimate public interest could be exposed using the role model argument.

It is also argued here that the correcting false impressions argument ought not to be a pivotal consideration for the English courts when determining the scope of Article 17(3)(a) or the journalism exemption. This factor has the potential to be widened in scope to a greater extent than the role model argument, as inventive counsel may argue that personal data ought to

[754] Elwood above, n 716 at 775.

remain online as it represents truths about a *private individual*, rather than someone in the public domain.[755] Indeed, personal information online often has the ability to expose details concerning the private lives of individuals, but such matters rarely relate to a matter of *genuine* public interest. Although a person may be anxious to have embarrassing information removed about themselves online, the data will seldom relate a matter of significant societal importance. The truth justification for free speech relies upon the notion that *it benefits society to be exposed to accurate information*. However, this is a generalised theory and does not take into account harm done to the reputation of individual data subjects whose personal information is released. As the ECtHR has observed, reputation is a consideration when seeking to balance privacy and expression interests, and this is something that the correcting false impressions argument fails to meaningfully take into account.[756]

iv. The right to criticise

The 'right to criticise' is the widest and most imprecisely framed of all public interest sub-factors. It advocates the freedom to critique others by revealing and commenting upon personal information about them,[757] its roots found within modern English precedent rather than Strasbourg jurisprudence.[758] It lacks a robust theoretical justification, other than that which states that the public's ability to criticise is essential to the development of society and contemporary debate. Precisely why critiquing mundane facts about a person's private life is vital to societal interests has not been explained by the English judiciary.[759] The right to criticise was borne out of the controversial case of *Terry and persons unknown*, which concerned a press exposé of the extra marital affair of John Terry, the then England football team captain. Mr Justice Tugendhat appeared to imply that the *potential* reliance on a 'defence' of public interest was enough to deny a privacy injunction,[760] before highlighting the valuable nature of the freedom to criticise modes of living.[761] Not only does this conflict with the earlier dicta of *Mosley*,[762] but also increases the likelihood of 'moral panics' and

[755] English and ECtHR privacy cases invoking the 'correcting false impressions' argument exclusively concern individuals who are in the public eye. See for example *Ferdinand, Campbell* and *Terry*.
[756] See, for example, *Lindon*.
[757] *Terry* [104] (Tugendhat J).
[758] Particularly within the case of *Terry*.
[759] *Terry* [104] (Tugendhat J).
[760] Wragg above, n 753 at 305.
[761] Ibid, 307.
[762] In which Lord Justice Eady sought to maintain a 'morally neutral' approach to privacy claims. See Wragg, Ibid, 307.

bolsters a culture of sensationalist journalism.[763] It is argued that information protected by the right to criticise may have even less public interest and genuine expression value than that of the role model and correcting false impressions factors. The latter two factors rely on the truth justification for free expression,[764] yet the right to criticise has no foundation in truth-seeking and appears to encourage gossip mongering under the guise that this is a societal good. The only traditional free speech justification the right to criticise could potentially rely upon is that of facilitating democracy, if the speech in question concerns a politician or someone running for elected office.

a. Application of 'the right to criticise' to the interpretation of Article 17(3)(a) and the journalistic exemption

Firstly, it should be noted that the right to criticise can be seen as simply an expanded facet of the *press as a watchdog* factor. Criticising those in authority is necessary (to an extent) as it creates an impetus for good performance, as was discussed earlier in this thesis. If the information in question concerns an elected official behaving badly, the right to criticise can rely on a similar justification to the watchdog factor but contains none of this factor's limitations. It can seemingly apply to criticising *anyone* about *anything*[765] as it has a basis in objective morality[766] and there is no precedent dictating that criticism has to be constructive. For these reasons, this factor unjustly prioritises speech over privacy and it is submitted here that it should not be considered by English (or European) judges interpreting Article 17's expression exception and journalism exemption. Not only does the factor appear to unfairly prioritise Article 10 but appears to bolster banal speech rather than important expression,[767] as it encourages comment upon the personal lives of individuals rather than issues of contemporary societal concern. Although encouraging public discussion about the furtherance of society has value, Wragg notes that broader societal issues can be discussed without reference to a person's private actions.[768]

[763] Ibid Wragg.
[764] Albeit marginally; the 'truth' in question relates to the personal lives of individuals, rather than matters of democratic or societal importance.
[765] Not just information disseminated online regarding someone in a position of authority. See Phillipson above, n 662 at 159.
[766] Wragg above, n 753 at 317 and *Terry*.
[767] Ibid Wragg, 313.
[768] Ibid, 312.

As highlighted above, the right to criticise is an argument adopted by the English courts and has little founding in ECtHR jurisprudence. The Strasbourg Court's approach within *Von Hannover v Germany* in particular is at odds with the broad-brush nature of this Article 10 consideration, as the Court stated that only matters of genuine public concern should be prioritised over an individual's privacy rights.[769] Phillipson has suggested that an unfavourable aspect of the right to criticise is that it enables a publisher (or in the context of Article 17, an online content-creator or website host) to decide whether to release personal data on the basis of their own moral code. This is inherently problematic due to the fact that moral codes are at best, context-dependent and at worst, arbitrary.[770] It can also be said that it is inappropriate for website operators[771] to adjudicate whether to act upon a deletion request as they have a vested interest in keeping a steady flow of information present on their webpages, as this maintains site popularity (and often a functioning business). A similar line of argument to this was engaged in by Lord Hoffmann in *Jameel*, his Lordship concluding that due to conflicts of interest 'newspapers are not often the best judges of where the line should be drawn' on what constitutes the public interest.[772] However, due to the currently limited lack of guidelines surrounding the operation of the right to be forgotten,[773] it appears likely that on an everyday basis data controllers will be expected to assess whether there is a public interest value in data which has been subject to an erasure request.[774] This would mean that the protection of privacy is at the mercy of an individual who embodies a conflict of interest regarding data flow online.

Additionally, the ECtHR has stressed the importance of responsible press behaviour when reporting on matters of legitimate public interest. Such responsibilities include that the press 'act in good faith and on an accurate factual basis and provide reliable and precise information.'[775] This appears to raise particular tensions within the right to criticise in online

[769] See *Von Hannover*. However, as discussed earlier, it is important to note that the Court has since shied away from its staunch protection of privacy rights within this judgment and delivered two judgments which appear to prioritise the expression of certain mundane facts about those in the public eye – *Von Hannover (no.2)* and *Von Hannover (No.3)*.
[770] Phillipson above, n 662 at 158.
[771] In other words, 'data controllers' for the purposes of the GDPR.
[772] *Jameel (Mohammed) and another v Wall Street Journal Europe Sprl* [2007] 1 AC 359 (HL), per Lord Hoffmann at [49] and see Phillipson above, n 662 at 140.
[773] More guidance will undoubtedly be released from national Data Protection Authorities in time.
[774] As they will likely be the first port of call for a data subject requesting deletion under Article 17 – they will have to decide whether or not to comply with this request.
[775] *Lindon* [67].

publications, as there has been an increasing trend towards 'citizen journalism' on the web as exposing a data subject's personal information.[776] The fact that user-generated critiques remain largely unregulated does not sit in accordance with the Strasbourg Court's repeated emphasis on the ethics of reportage. The court has gone so far as to say that Article 10 protection would *not* extend to cover irresponsible or unprofessional publications in wake of a competing privacy claim:

> '…the safeguard afforded by Article 10 to journalists in relation to reporting on issues of general interest is **subject to the proviso** that they are acting in **good faith in order to provide accurate and reliable information** in accordance with the ethics of journalism'.[777]

It is argued here that freedom of expression in the form of the Article 17(3)(a) exception should not be extended to automatically cover content produced by citizen journalists on the internet, as there is currently little moderation of blogs and other exposé sites regularly divulging personal information online. Much content is therefore not checked for accuracy or adequately contextualised, leading to misleading representations of a data subject being circulated online.[778] To add to this problem, the pieces of personal information that a gossip site may choose to comment upon are those which are likely to be controversial or sensational. This can lead to discrete pockets of personal data available online which may be an inaccurate overall reflection of an individual's true personality.[779] Finally, the right to criticise conflicts with theoretical justifications for the protection of privacy; including that which states privacy allows an individual to make their own mistakes in solitude, free from the judgement of others.[780] If an individual is living in fear of their experimentations (in either their personal or professional life) being a matter of public record, this will lead to

[776] See for example, sites such as 'Guru Gossip'; accessible at: https://gurugossiper.com/ (last accessed 7/4/19). Gossip websites such as these encourage discussions of the personal lives of others and some users post private information about those discussed to these public domains.
[777] *Bladet* [emphasis added].
[778] See generally Daniel Solove, *The Future of Reputation* (Yale University Press 2007) and *Delete,* 90.
[779] Ibid.
[780] See articles such as Jeffrey Rosen, 'Why Privacy Matters' (2000) 24(4) *The Wilson Quarterly* 32, 38 and Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89(3) *The Yale Law Journal* 421 and Phillipson above, n 662 at 160 also see Chapter 2 of this thesis.

individuals censoring themselves and constraining their own innovation. This has negative effects not only on the personal autonomy of an individual but on society as a whole.[781]

b. Recent developments in the right to criticise

In May 2016, the UK Supreme Court decided the case of *PJS v NGN Ltd*.[782] The case concerned the husband of a famous celebrity (they have two young children), who was seeking to prevent a publication by the defendant newspaper of details concerning his involvement in an extra-marital threesome, on the grounds of misuse of private information (and Article 8 ECHR).[783] The court granted the injunction.[784] The Supreme Court in its judgment quashed the notion of the 'right to criticise' as an argument in favour of the disclosure of private information. Lord Mance held:

> 'The Court of Appeal in my opinion also **erred** in the reference it made…to there being in the circumstances even a "limited public interest" in the proposed story…In identifying this interest, the Court of Appeal relied upon a point made by an earlier Court of Appeal in the *Hutcheson case [2012] EMLR 2* (and before that by Tugendhat J in the *Terry case [2010] 2 FLR 1306*), namely that the media are entitled to criticise the conduct of individuals even where there is nothing illegal about it…**criticism of conduct cannot be a pretext for invasion of privacy by disclosure of alleged sexual infidelity which is of no real public interest in a legal sense**.'[785]

This statement from Lord Mance (supported by the majority in the Court) unequivocally discredits the *Terry* case's stance with regards to the right to criticise as well as the factor on its own terms. Lord Mance makes it clear here that the notion of *criticism for criticism's sake* does not give rise to a legitimate public interest, absent of other relevant factors.[786] This firm stance will silence commentators who have argued that after *Terry*, the right to criticise is a new consideration of the courts when weighing up competing interests in expression and

[781] See chapter 2.
[782] (2016) AC 1081.
[783] (2016) AC 1081.
[784] However, articles relating to the claimant's affairs were published in Scotland and in the US (jurisdictions not covered by the injunction). Despite the injunction, it was relatively easy to find the name of the claimant/couple on social networking site Twitter, with many people tweeting with reference to the claimant's husband's occupation in the entertainment business.
[785] *PJS v NGN Ltd* (2016) AC 1081, 1095 (Lord Mance) [21 – emphasis added].
[786] This was discussed in detail by Gavin Phillipson in his presentation, 'Threesome injuncted: has the Supreme Court turned the tide against the media in online privacy cases?', *IALS Annual Conference: 'Restricted and Redacted'* (9 November 2016).

privacy.[787] It is difficult to predict if this factor will be resurrected within caselaw in the future[788] but the judgment of Lord Mance here is to be welcomed.[789] The above section of this thesis has provided two reasons for the English courts to abandon this balancing factor in relation to Article 17 and it now appears that the English courts are also attempting to distance themselves from the problematic judgment of *Terry*.

v. The passage of time and the public interest

The above four Article 10 balancing factors are perhaps the most frequently used arguments that pervade expression jurisprudence. However, there are other factors besides these which occasionally are employed in assessing the importance of expression by the Strasbourg and English courts. One of these less prominent factors which is sometimes present in Article 10 caselaw is *the amount of time passed* between an event and its reportage. This passage of time can impact upon whether the ECtHR deems that a publication has a public interest value which overrides privacy rights. The most pertinent example of this is in *Plon (Societe) v France*, which concerned the publication of information concerning the health of a former French president (who was deceased). In finding that Article 10 interests prevailed over privacy rights of the late minister's family, the Strasbourg Court noted that a significant fact was the amount of time that had expired between the president's death and the publication of the material.[790]

a. Application of 'the passage of time' factor to the interpretation of Article 17(3)(a) and the journalistic exemption

It is argued here that although *a significant amount of time amassed* between information as first posted and subsequently requested for deletion may be a relevant factor when interpreting Article 17, it ought not to be a *pivotal* consideration for the courts in terms of 'tipping the balance' in favour of expression. Indeed, it may often be the case that the greater

[787] This in particular has been expounded by Paul Wragg, although he is not in favour of the 'balancing factor': see above, n 753.
[788] Although this is not beyond the realms of possibility; English common law has a long history in all legal fields of generating contradictory precedent.
[789] *PJS* will be discussed in detail in the next chapter regarding misuse of private information.
[790] *Plon (Societe)* above, n 752 and see Mowbray above, n 664 at 580.

the amount of time that has elapsed – and the more irrelevant data has therefore become – the more likely it is that a data subject will want the information 'forgotten'. For example, this could be the case with personal data available online that reveals that an individual has, at some prior point in their life, had a house repossessed. That individual may have subsequently restored their financial stability and be seeking to invoke the right to be forgotten in order to move on from this time in their life.[791] This correlates directly with the theoretical justification of privacy as allowing an individual to move on in their lives, encouraging personal autonomy and the ability to change lifestyle. However, personal information that has been posted online even contemporaneously can have the effect of negatively impacting a data subject's life. If a compromising picture of an individual is uploaded to a social networking site this has the potential to be viewed by their friends, lovers, co-workers and colleagues *immediately*. Depending on the nature of the image, instant negative ramifications could arise from this both socially and professionally. Due to this, it is argued here that despite above dicta from the Strasbourg Court, the *passage of time* should not be a decisive factor for the judiciary when assessing the scope of Article 17's expression exception or journalistic exemption.

vi. The public interest in crimes

Another less prevalent but nevertheless interesting Article 10 balancing factor that ought to be briefly discussed is the 'public interest in crimes.' There is a clear trend in ECtHR jurisprudence of the prioritisation of Article 10 interests over privacy rights in relation to the publication of details exposing crimes. This is justified by the court through a public interest in the reportage of criminal acts and wrongdoing, as was argued in *Axel Springer*.[792] It is also justified in the English courts by virtue of a criminal offence being a matter of public record – an offender cannot expect privacy in relation to the commission of such an offence for this reason.[793] In addition, freedom of expression also tends to be given priority in relation to the reportage of on-going trials in good faith.[794]

[791] This is a deliberate (but approximate) parallel to the circumstances surrounding the case of *Google Spain.*
[792] *Axel Springer.*
[793] See below, *NT1 and NT2.*
[794] *Erla Hlynsdóttir v. Iceland (no. 3)* App no. 54145/10 (ECHR, 2 June 2015).

a. Application of 'the right to criticise' to the interpretation of Article 17(3)(a) and the journalistic exemption

It is argued here that the reportage of crimes is indeed something that will likely fall to be protected under Article 17(3)(a)'s expression exception, journalism exemption or other exemption.[795] Despite this, attention ought to be paid by the English courts to data subjects requesting deletion of information relating to their previous *minor*[796] criminal offences. In these circumstances deletion requests ought to be duly considered; the ability of an individual to reform themselves into a law-abiding citizen is of fundamental societal importance.[797] Indeed, the ability to do so has been codified into statute by the Rehabilitation of Offenders Act 1974.[798] If documentation of the prior illegality of such a person remains present online, it can be difficult for the individual to 'move on' in their new life and put their past behind them. As discussed earlier in this thesis, the ability to forget is a human function enabling an individual to move forward and reconstruct himself or herself for the better. The 'total recall' capabilities of the internet interfere with this important psychological function, by solidifying events that would previously have been forgotten in its 'perfect memory' as forever accessible. If Article 17 is to readdress the balance between remembering and forgetting online, deletion of data regarding past minor deviances must be considered to fall within its ambit.[799]

As noted above, the first English 'delisting' case of *NT1 and NT2* concerned two data subjects requesting the deletion of links to websites which detailed their past criminal

[795] For example, Paragraph 5(3), schedule 2 of the Data Protection Act 2018 states that: 'the listed GDPR provisions do not apply to personal data where disclosure of the data… is necessary for the purpose of, or **in connection with, legal proceedings** (including prospective legal proceedings)'. This could potentially exempt the right to erasure in this scenario.
[796] This however, ought not to apply to serious criminal offences – for example, historical sex abuse. The Sex Offenders Register in the UK (which records individuals who have been convicted of sexual offences) plays a crucial part in society in protecting children from past offenders in the present day. It is however beyond the scope of this thesis to compile a list of what crimes, and the reportage of which, should or should not be allowed to be erased under Article 17. This is something to be considered in practice and on an individual case basis.
[797] See generally *Delete.* Mayer-Schönberger argues that forgetting is a fundamental facet of healthy society, allowing people to live in the present.
[798] Rehabilitation of Offenders Act 1974.
[799] De Mars and O'Callaghan have argued that the memory capabilities of the internet are what makes the right to be forgotten necessary in contemporary society. See Sylvia de Mars and Patrick O'Callaghan, 'Privacy and Search Engines: Forgetting or Contextualising?' 43(2) *Journal of Law and Society* 257, 258. Also see *Delete.*

convictions.[800] Both men had been found guilty for criminal offences in the past and served jail-time – and both were entitled to rehabilitation under the Rehabilitation of Offenders Act 1974. Lord Justice Warby in the case observed that there was an interaction between the Data Protection Act 1998 and the Rehabilitation of Offenders Act, and that part of an offender's rehabilitation was a right to privacy (under Article 8 ECHR).[801] However, Lord Justice Warby reasoned that the rehabilitation of offenders is only a 'qualified right' and can conflict with freedom of expression, and that an offender cannot have a reasonable expectation of privacy if they are subject to criminal proceedings.[802] The judge also noted that the Act does not mean that a person is guaranteed *complete* privacy regarding their spent conviction but this *will* be a weighty factor in favour of their privacy rights, due to the potential negative repercussions of revealing that information for the person concerned.[803] In the case, Lord Justice Warby found against one claimant's delisting requests (NT1) and for another's (NT2). This decision largely hinged upon both claimants' behaviour since their convictions had become spent. NT1 had sought to falsely present himself as a clean-cut businessman despite his conviction for a dishonesty offence, whereas NT2 had pleaded guilty to his offence and shown remorse.[804] In addition, the judge found it relevant that NT2's conviction was always going to become spent (it was for a less significant crime than NT1's), whereas NT1's conviction only fell under the remit of the Rehabilitation of Offenders Act because of a recent change in the law.[805] It appears, then, if this case is followed in future with regards to the Data Protection Act 2018, that the Rehabilitation of Offenders Act *can* work, in some circumstances, to bolster a deletion right – dependent upon other factors within a case.

Conclusion

This chapter has argued that what constitutes information in the 'public interest' is best assessed through the benefit of an audience from receiving certain pieces of information in balance with the harm caused to a data subject of the personal data as public. If there is a significant benefit to an online audience in comparison with the loss of personality rights to the individual concerned, then Article 17(3)(a) or the journalism exemption should, in some cases, be operable. The crux of the matter is whether there is a *genuine* public interest in the

[800] *NT1 and NT2*. It should be reminded here that this case was decided before the enforcement of the GDPR and the Data Protection Act 2018.
[801] *NT1 and NT2* [166].
[802] *NT1 and NT2* [166].
[803] *NT1 and NT2* [166(2)].
[804] *NT1 and NT2* [169] and [203].
[805] *NT1 and NT2* [167].

information as disclosed; if there is, then this must be seriously taken into account in a court's assessment and weighed against the reputational harm done to a data subject through the disclosure.

This and the previous chapter have sought to examine Article 17 using Articles 8 and 10 ECHR as a normative framework. They have suggested ways in which the English courts ought to interpret the new right so that it complies with the standards set by the Strasbourg Court and in a manner which champions informational control online. It has been necessary to directly apply the caselaw of the ECtHR here to Article 17 as the right has not necessarily been drafted with the ECHR in mind, as it is born out of an EU Regulation and is broadly drawn in the GDPR's text. The above two chapters have offered guidance as to how precisely the English courts should construe an erasure request in order to solve the problem identified by this PhD: a lack of data privacy online. The thesis will now move on to examine misuse of private information – and to what extent it has been able to tackle a lack of privacy rights online.

Chapter 5: Domestic 'privacy' law and its efficacy in protecting personal data online

Introduction

This chapter discusses the common law 'privacy tort,'[806] of misuse of private information (hereafter 'MPI'). This is the strongest cause of action with respect to informational privacy currently available in England and Wales and allows injunctive relief to be obtained – the strengths and pitfalls of which will be discussed in the last section of the chapter. Although the 'right to be forgotten' enables a data subject to request the deletion of content online, it is an *ex post* remedy; the information may have already caused harm by initially being posted online. Injunctive relief has the potential to stop certain material being published at all. Therefore, on an initial assessment, MPI can provide protection for private information and has in fact done so in various cases. However, this chapter will argue that in some aspects, MPI has proven to be ineffective – especially in relation to online privacy – for several reasons, which will be evaluated by making reference to the 'data dissemination scenarios' (outlined above in the introduction).

The first reason is that generous treatment has been given by the English courts to press freedom while adjudicating on some MPI cases. In certain cases, broad interpretations of what constitutes the 'public interest' on the part of the courts have been damaging in some instances to claimants seeking to assert their privacy rights.[807] These interpretations in particular judgments have in effect legitimised the publication of banal facts about a person's private life, despite the information in question having little or no *genuine* public interest value.[808] This has had a negative effect on the right to informational privacy and its

[806] Although the court in *Wainwright* in 2004 was at pains to state that there was no general English tort of invasion of privacy (*Wainwright v Home Office* [2004] 2 AC 406 [28-35]), the court in *Campbell* confirmed that in light of their obligations under the Human Rights Act 1998 section 6 that there is an English action against unauthorised disclosure of private information which should be referred to as the tort of 'misuse of private information' (*Campbell* [14]). It must be noted that *Wainwright* was not concerned with information: the tort is much narrower than Article 8 itself which covers all sorts of invasions of 'privacy'. Obviously, breaches of Article 8 can be claimed under the Human Rights Act against public authorities, but the common law MPI action does not cover all such breaches.

[807] Particularly in the cases of *Terry* and *Ferdinand*. It should be noted that this may not be a problem which is unique to MPI – unfortunately, there is a chance that the English courts will interpret the public interest in an expansive manner when adjudicating on erasure claims concerning celebrities in the future. However, they would likely not take this approach with regards to private individuals.

[808] See chapter 4 of this thesis that concerns the Strasbourg courts' interpretation of the scope of Article 10 ECHR and the public interest.

importance in England and Wales.[809] In a general sense, certain broad readings of the public interest has undermined efforts to assert the importance of privacy in the digital age, although there is some evidence to support the notion that a more privacy-friendly approach has recently been adopted by the English judiciary, as will be discussed below.[810]

Secondly, a doctrine of 'waiver' has been used in a group of MPI cases, under which a claimant is seen as having 'waived' their privacy rights by disclosing some aspect of their private life in the past to the public at large (to a greater or a lesser extent). Therefore, on some readings of this principle MPI cannot be relied upon by an individual who has voluntarily disclosed information from a certain 'zone' of their private life and later wishes to protect information within that zone from publication. The modern prevalence and relevance of waiver as a factor will be questioned in this thesis – it should be noted that certain contemporary MPI judgments do not discuss waiver at all, so its application by the courts as a factor has been inconsistent.

Thirdly, the notion of 'public domain' has similarly evolved in MPI jurisprudence as a caveat to finding that a 'reasonable expectation of privacy'[811] exists. The public domain doctrine has traditionally stated that if the personal information is already known to the public (to an extent the court deems significant) then the information has lost its private quality and may be no longer protected. The application of the notion of the public domain has also been called into question by the decision of *PJS*, which will be discussed at length in this chapter.[812] The public domain doctrine *could* work to negate an MPI claim with regards to information widely disclosed online on a publicly accessible website[813] potentially applicable to all of the above data dissemination scenarios.

[809] These interpretations, which will be discussed in detail below, took the English courts actively 'backwards' in the sense that far from its prior assertion that Articles 8 and 10 have equal value (*Re S* [2004] UKHL 47 [para.17 per Lord Steyn]) they seemed to suggest that Article 10 may take precedence over Article 8, a position symptomatic of the English courts' pre–Human Rights Act jurisprudence.
[810] See *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26 hereafter '*PJS*' and *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC), hereafter '*Sir Cliff*'.
[811] On behalf of the claimant – the first requirement of successful misuse action.
[812] In which the information being released online and in certain print publications outside of the jurisdiction did not negate an injunction being granted in respect of the information.
[813] C/f *PJS*, in which the Supreme Court held that the public domain doctrine did not inhibit an interim injunction being awarded – despite the fact that the personal information in question had already been disclosed widely on and offline in other jurisdictions.

Finally, an argument will be put forward below that MPI's two remedies of injunctions and damages are ineffective in practice, and are particularly problematic in relation to private information disseminated online. Firstly, if an injunction suppressing publication is granted to a claimant[814] it can be difficult to prevent web-based dissemination where no specific person or body can be identified as a poster.[815] An injunction is also unable to inhibit publication (including that online) outside the jurisdiction. Indeed, in recent caselaw the discussions of injunctions have concentrated on stopping further harm being done by dissemination inside the jurisdiction rather than their inability to make an impact outside of it.[816]

These difficulties with MPI mean that it is not often able to provide an adequate remedy for data subjects. Each strand of argument will be discussed in detail below. It is important to note from the outset that MPI has been shaped in a particular way due to its origins – it was created primarily to guard against large newspaper conglomerates seeking to profit from the publication of private facts about celebrities.[817] MPI as a tort must be observed through this lens, as this gives a better understanding as to why it is ill-equipped to deal with private individuals seeking to remove personal data from social networking or other sites.[818] As will be discussed below, MPI was born out of the traditional action for breach of confidence, which centres upon the unauthorised disclosure of confidential information in breach of an express or implied duty of confidence.[819] It therefore should come as no surprise that MPI is unable in most circumstances to offer a route to redress for personal data *voluntarily* uploaded online by the data subject herself (in the *personal public disclosure* scenario). Both notions of waiver and the public domain also originate from jurisprudence relating to the interpretation of breach of confidence.

Again, Articles 8 and 10 ECHR provide the normative backdrop for this chapter's analysis. However, as explained earlier in this thesis, the principles taken from the ECtHR caselaw discussed in the previous two chapters will not be repeated here. MPI has been created and

[814] And a fight to acquire one can be difficult in of itself.
[815] This is a pitfall which Article 17 may avoid, as if the post is on a social networking site (and the site is deemed jointly and severally liable as a controller), then a data subject could request that the site deletes this information.
[816] See *PJS*, where the information in question had been published extensively in, for example, the US. Analysis of this case in respect of injunctions will be returned to later in this chapter.
[817] Jacob Rowbottom, 'A landmark at a turning point: Campbell and the use of privacy law to constrain media power' (2015) 7(2) *Journal of Media Law* 170, 184.
[818] Ibid.
[819] See Gavin Phillipson and Helen Fenwick, 'Breach of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 *Modern Law Review* 660.

developed by the English courts to accord with the requirements of Article 8, due to the obligations imposed by the Human Rights Act 1998. As will be discussed below, the creation of a balance between Articles 8 and 10, especially in the Supreme Court in *PJS*, provides a model for the creation of such a balance under the Data Protection Act 2018, so long as the failures to accord the Articles equal weight in some instances to be discussed are avoided.

This chapter seeks to answer research question 2 as outlined in the introduction*: 'Are any areas of English tort law able to effectively protect an individual's personal data rights, especially online, while balancing interests of freedom of expression?'*. This chapter will argue that placing a focus on the deficiencies of MPI in terms of addressing privacy harms online demonstrates the strength of the argument for heralding the advent of the GDPR as providing a far more effective means of addressing such harms.

A. The origins of the tort of misuse of private information

As English law stood prior to the year 2000 – before the coming into force of the Human Rights Act 1998 (hereafter 'HRA') – there was an equitable remedy for breach of confidence, but it was not akin to a tort of privacy.[820] There were three requirements to satisfy a breach of confidence action: i) the information at issue must have a quality of confidence, ii) it must be imparted in a relationship of confidence and iii) the receiver of the information must then use it in an unauthorised way.[821] After the Human Rights Act came into force, breach of confidence 'gave birth' to the new tort of MPI. This was arguably a necessary step for the courts to take, as the effect of both section 3 and 6 of the Human Rights Act is to place an obligation on the courts as a public authority to interpret relevant national law in harmony with Convention rights – including Article 8.[822] Section 2 of the Human Rights Act was also relevant to the Court's decision to expand the law in this way; section 2 provides that judgments of the Strasbourg Court are relevant to domestic jurisprudence, meaning that a

[820] *Wainwright v Home Office* [2004] 2 AC 406 [28-35].
[821] *Coco v AN Clark Engineers Ltd* [1969] RPC 41 [47] and *Malone v Commissioner of Police of the Metropolis* (*No.2*) [1979] Ch.344 [375]. See Simon Deakin, Angus Johnson and Basil Markesinis, *Tort Law* (6th Edn, OUP 2012) 838.
[822] Section 3 Human Rights Act 1998 states that: 'So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights' and section 6 states that: 'It is unlawful for a public authority to act in a way which is incompatible with a Convention right' – the courts are a public authority under section 6(3)(a) of the Act.

large body of ECtHR caselaw concerning Article 8 and 10 rights could infuse and re-shape the existing action for breach of confidence.[823]

A string of caselaw can be charted to map the creation of MPI: intimations of imminent change were present within *Douglas and Zeta Jones and ors v Hello!*[824] in 2001 where Lord Justice Sedley found in favour of Catherine Zeta-Jones' and Michael Douglas' privacy rights under Article 8. A year later the notion of a 'reasonable expectation of privacy'[825] as the basic test for the developing action was proffered in *A v B Plc*.[826] This shift culminated in the seminal case of *Campbell v MGN* in 2004, which named the new tort.[827] In *Campbell*, the House of Lords can be seen as moving away from the analysis of whether the information (in this case, photographs) was confidential to focusing upon the harm done to the claimant through publication.[828] Rowbottom has noted that the Lords in the case moved from a confidence-based discussion to that of a human rights assessment, focusing upon autonomy and dignity.[829] One matter that has been made clear by the courts is that MPI is a separate tort to breach of confidence,[830] although breach of confidence elements can bolster an action in MPI.[831] This has been confirmed in the recent case of *Sir Cliff Richard*.[832] Here, information about a historical sex abuse investigation into Sir Cliff Richard had been provided to the BBC from a source inside the highly confidential Operation Yewtree.[833] Mr Justice Mann held that the BBC journalist at the centre of the matter should have known that the information was 'confidential and sensitive' prior to publication and that although this did not mean that Article 10 rights could be dismissed, it did weaken the BBC's position in the case.[834]The action of MPI is now clearly an informational privacy tort.

B. Outlining the elements of MPI; initial criticisms

[823] Section 2 of the Human Rights Act 1998 provides that a court or tribunal must take into account decisions of the European Court of Human Rights when making its assessment.
[824] [2001] 2 All ER 289.
[825] Rather than pin-pointing a relationship of confidence.
[826] *A v B Plc* [2002] *3 WLR 542*, [551B].
[827] *Campbell* [14] (Lord Nicholls).
[828] Deakin, Johnson and Markesinis above, n 821 at 844.
[829] Rowbottom above, n 817 at 171.
[830] *Google Inc v Judith Vidal–Hall* [2015] E.M.L.R. 15, [2015] E.W.C.A. Civ 311.
[831] *HRH Prince of Wales v Associated Newspapers* [2006] EWCA Civ 1776 and *McKennit v Ash* [2006] EWCA CIV 1714.
[832] *Sir Cliff*.
[833] *Sir Cliff* [290].
[834] *Sir Cliff* [292].

The tort is comprised of two parts: firstly, the claimant must show that they had a reasonable expectation of privacy in relation to the information disclosed. If this is successfully made out, then the court moves to a 'balancing exercise' also termed the *parallel analysis*, where it weighs Article 8 privacy interests against competing Article 10 expression factors. Even at first glance, it is easy to observe that these two exercises lack structure. As a result, sub-tests have developed at both stages of the decision procedure in an effort to make the action more coherent. While establishing whether a reasonable expectation of privacy exists, the courts have created a range of considerations that can be taken into account, such as: the attributes of the claimant, the nature and purpose of the intrusion, the location of the photographs (if photographs are involved), the absence of consent and the effect of publication on the claimant.[835] This range of considerations has also been affirmed in 2018 in *Sir Cliff Richard*, where the Court also made reference to the ECtHR case of *Axel Springer*, which includes analysis of the above factors.[836]

Despite these guidelines, it is clear that the test is still 'broad and general'.[837] It could be said that establishing a reasonable expectation of privacy is an intuitive analysis and extremely fact–specific, so an attempt to artificially create a test surrounding it was a reductive exercise, and was certainly never designed to be comprehensive. The parallel analysis exercise also involves several sub-factors which leads to Article 8 or 10 winning out; this includes whether the information is in the public interest and the level of intrusion suffered by the claimant.[838] Moosavian has observed that this balancing exercise is also inherently unclear:

> 'Thus perhaps "balance" acts as a convenient fiction which overlays an inherently creative, subjective and, to some extent, inexpressible interpretive activity…'[839]

[835] *Terry* [55]. This list of considerations accompanies a 'reasonableness' test on the part of a claimant.
[836] *Sir Cliff* [276] and *Axel Springer*.
[837] Jojo Y.C. Mo, 'Misuse of private information as a tort: The implications of Google v Judith Vidall-Hall (2017) 33 *Computer Law and Security Review* 87, 92.
[838] See for example, *David Murray v Express Newspapers* [2007] EWHC 1908 (Ch) and *Murray v Big Pictures* [2008] EWCA Civ. 446 [61] regarding press intrusion and *Ferdinand* and *PJS* [24] for a detailed discussion of what may constitute the public interest.
[839] Rebecca Moosavian, 'A just balance or just imbalance? The role of metaphor in misuse of private information' (2015) 7(2) *Journal of Media Law* 196, 217. Wragg similarly argues that parallel analysis relies upon 'abstract terms' but he only considers the negative effects of this upon freedom of expression – he fails to grasp that this may also negatively impact privacy rights. See Paul Wragg, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) *Journal of Media Law* 225, 234.

Wragg has gone further and argued that the balancing exercise is so vague that it fails to give judges any tools with which to affect the balance.[840] Although the balancing exercise can (and should) be critiqued, this is, it is argued, an overstatement of its problems. In particular, Strasbourg case law such as *Von Hannover* (*no.2*) has provided a partial framework with regards to adjudicating between Articles 8 and 10, noting the importance of whether the claimant is a celebrity, the subject of the publication and the consequences of the disclosure, among other principles.[841] This approach has been followed in English cases such as *Weller*.[842] It is important to remember that the MPI action of misuse has been 'forged' with traditional mass-media actors in mind.[843] Although Wragg's analysis over-states the problem, it is nevertheless argued that the balancing exercise lacks clarity, predictability and certainty, as elaborated upon below. It at this point, remains unclear as to whether a balancing exercise conducted under Article 17 in the English courts will be any more or less structured than that which has come before it with regards to MPI. Given the increasing role that Data Protection Authorities have been awarded under the GDPR (as well as impetus to work together),[844] there is reason to believe that a more detailed balancing structure may be drawn up for usage in this regard and implemented across Europe – indeed, Article 29 Working Party has in the past issued a table detailing balancing factors (geared towards private data online), and how they might be used. It is submitted here that some of the pitfalls that the English courts have fallen into with regards to parallel analysis in MPI ought to be avoided with regards to balancing privacy rights under Article 17 – this will be discussed below.

Moralistic factors have crept into MPI's balancing exercise, which could in part account for its lack of precision.[845] It is possible that judges have intentionally included morality in the exercise or it may simply be a result of the types of MPI cases that have gone to trial.[846] It could also be in part due to the breach of confidence roots of the tort, given that breach of confidence is an equitable action. An example of such morality can be seen in the judgment of *A v B, C and D* in 2005.[847] The case concerned the notion of 'zonal waiver' – in other

[840] Paul Wragg, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) *Journal of Media Law* 225, 229.
[841] *Von Hannover (No.2)* [108-113].
[842] *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB), [2014] E.M.L.R. 24.
[843] Rowbottom above, n 817 at 187.
[844] See chapter 3, part I.
[845] Such as the emphasis the courts have placed on disclosing sexual affairs outside of marriage, despite the fact no legal wrong has been committed. See both *Terry* and *Ferdinand*.
[846] Many high-profile cases have concerned extra-marital affairs and other forms of sexual deviancy.
[847] *A v B, C and D* [2005] EWHC 1651 (QB); [2005] EMLR 851 [28].

words, that a claimant may waive their right to privacy by disclosing information of a similar type to that which is the subject of the claim, in the past.[848] In this case it was held that because the person in question had disclosed information about their drug-taking in the past, further disclosure about *other* details of their drug taking did not invoke any Article 8 protection. This is *despite* the fact that the judgment acknowledged that circumstances may change and what is designated a *zone of information* may be wide:

> '…a drug addict, or former addict, who has chosen to speak about his past experiences is not necessarily precluded thereafter, on a once for all basis, from seeking protection in respect of other experiences. Suppose he had chosen to speak about his addiction and the unpleasant experiences he had suffered in the past, and recounted how he had overcome his addiction. If he were later to lapse, it would not necessarily follow that his new health problems would also automatically be open to media intrusion.'[849]

Contrary to the above reasoning, the judge held in the case that further disclosures of personal information about the subject's drug taking was merely 'more of the same'.[850] This appears illogical, as the information in question, although still on the subject of drug taking, was new – much as the information in the example given above regarding a relapse would be new. This leads one to question the true reason for the outcome of the case, and whether the judge was more convinced that the data in question didn't deserve privacy-related protection because the private information pointed to - arguably - 'immoral' behaviour on the part of the claimant.[851] Regardless of *why* morals have been considered in this balancing exercise, their inclusion can be criticised. A concern in this regard considers what the 'correct' version of morality should be, and whether judges are able to be representative in their assessment of this, taking into account minority views. In a more general way, the inclusion of morality into privacy judgments is problematic since if the balancing exercise purportedly concentrates on issues such as the public interest, arguably an emphasis should be placed on defining a genuine matter of public interest rather than what constitutes moralistic behaviour.

[848] This case (and 'waiver' more generally) is discussed below.
[849] *A v B, C and D* above, n 847 [29].
[850] Ibid [30].
[851] For more detailed examination of how morality is present in parallel analysis within privacy caselaw, see chapter 4 of this thesis, which examines this trend in English and Strasbourg jurisprudence concerning Article 10.

The English judiciary have attempted to deliver definitive decisions in MPI cases; however they are often compromised by a heavy use of metaphor.[852] The other name for parallel analysis, 'the balancing exercise', is a metaphor in of itself: it envisages a weighing scales of Article 8 rights on one side and Article 10 interests on the other. The English courts rely on this balancing exercise, speaking with authority in judgments that it provides a definitive answer as to the success of a claim. Lord Steyn says of the balancing exercise:

> 'First, neither article [8 and 10 ECHR] has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an *intense focus* on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justification for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each.'[853]

Although this appears to provide a decisive guiding structure, much about the balancing exercise is left unsaid. How many 'factors' are needed to tip the scale? The metaphor fails to tell us. Would a certain factor as present on one side of the scale be enough? Does 'public interest in publication' always weigh heavier on the scale than 'intrusion' on a claimant? Although the metaphor for a balance or weighing scale here may be a convenient description, it casts little light on the specifics of the exercise itself and may raise more questions than it answers. The above quotation introduces another turn of phrase: an 'intense focus on the facts' as paramount to Article 8-10 balancing. Again, this is a definite statement, undoubtedly made by Lord Steyn in an attempt to give some guidance as to the parallel analysis. However, if one pauses to consider this inclusion, it adds little to our understanding of how the exercise is conducted. Surely, reference to the factual context of a case is a given – without such consideration, a judge would not be able to assess which factors on either side of the balance were at play. The resounding point from these two examples is that the language used within misuse of private information jurisprudence can serve to disguise the lack of coherent principle within the tort. At this point, it remains unclear as to whether the English courts will issue judgments laced with metaphor when balancing rights under an Article 17 claim (according to the Data Protection Act 2018), or attempt to create a more structured approach

[852] Moosavian above, n 839 at 215.
[853] *Re S (A Child)* [2005] 1 AC 593 [17].

with help from national Data Protection Authorities across Europe. It seems unlikely that the English courts, while adjudicating on the right to erasure, will cease to use metaphor altogether – as it is likely that they will draw heavily on MPI judgments in order to make decisions in this regard, as it is arguably the closest legal instrument which currently exists in English and Welsh law. This problem of metaphor therefore may persist. Rowbottom argues that there are a number of ongoing debates concerning MPI,[854] but the most important matter to consider for present purposes is whether MPI is effective in light of the rise of social media. It is this which will be discussed below.

C. The erratic treatment of press freedom in MPI's caselaw

The former section of this chapter aimed to give a general introduction to MPI and its origins in order to give context to its problems and inadequacies. As the introduction to this chapter has outlined, there are several flaws with the tort that render it ineffective in protecting privacy rights. The first that will be discussed here is the erratic and unpredictable nature of MPI judgments and their prioritisation of press freedom. In some of the English and Welsh courts' most notable privacy cases, privacy-expression balancing has led to the prioritisation of privacy interests, and balancing has at least appeared 'fair'. Namely, in the seminal case of *Campbell*, the supermodel's privacy rights won-out over press freedom factors – the judgment taking place in the House of Lords. The decision in *Campbell* was a trailblazing case, which, as stated above, due to the Human Rights Act 1998 *de facto* created a tort of privacy in England and Wales.[855] Indeed, Lord Nicholls in *Campbell* stated:

> 'This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship. In doing so, it has changed its nature.'[856]

This was a significant step forward for privacy rights in England and Wales, and in the case Baroness Hale articulated a 'reasonable expectation of privacy test' which could be utilised by the English courts to assess whether a claimant would be successful in their MPI claim.[857]

[854] For example, does it encompass too much information or not enough?
[855] Gavin Phillipson, 'Transforming Breach of Confidence? Towards A Common Law Right of Privacy Under the Human Rights Act' (2003) 66 *Modern Law Review* 726, 726-728, also see *Wainwright v Home Office* [2004] 2 AC 406 [28-35].
[856] *Campbell* [14].
[857] Ibid [135].

Despite the fact the photographs in question of the claimant were taken in a public street, consideration was given by the Court to the fact that she felt hounded by the press (mirroring the ECtHR's judgment in *Von Hannover*).[858] Most notably, Lord Nicholls argued that disseminating information about the claimant's attendance at narcotics anonymous meetings was of a 'lower order' than other forms of journalistic speech - such as political speech – [859] and that photographs 'contain more information' about a subject than text alone.[860]

Another high-profile case which found in favour of privacy rights is *McKennitt v Ash*, decided a few years after *Campbell*. Here, an injunction was upheld prohibiting the publication of a book detailing certain aspects of the private life of a Canadian folk-singer, Loreena McKennitt. The case was of a different nature to *Campbell* – it turned on a *relationship of confidence* between the folk singer (who was the subject of the book – an unauthorised biography) and the book's author. Breach of confidence, the old-fashioned root of MPI was therefore central to the case. Indeed, Lord Justice Buxton noted that:

> 'of great importance in the present case, as will be explained further below, the complaint here is of what might be called old-fashioned breach of confidence by way of conduct inconsistent with a pre-existing relationship'.[861]

Nevertheless, the case highlighted the importance of protecting informational privacy. Like *Campbell*, the decision in *McKennitt* was profoundly influenced by the ECtHR's judgment of *Von Hannover*, a decision which itself robustly prioritised the Article 8 interests of Princess Caroline of Monaco over competing freedom of expression arguments.[862] Lord Justice Buxton set great store by the ECtHR's balancing exercise between Articles 8 and 10, stating:

> 'In order to find the rules of the English law of breach of confidence we now have to look in the jurisprudence of articles 8 and 10.'[863]

This pro-privacy ruling was, perhaps unsurprisingly, criticised by the mainstream media at the time; the BBC noting that an English right to privacy had been created out of breach of

[858] Ibid [30]
[859] Ibid [29].
[860] Ibid [31].
[861] *McKennitt v Ash* above, n 831 at [11].
[862] Ibid [41].
[863] Ibid [11].

confidence and that the decision would deal a blow to publishers seeking to sell similar books – the decision 'puts pressure on celebrity books'.[864] Also in 2006, the Court of Appeal delivered the judgment of *HRH Prince of Wales v Associated Newspapers Ltd*.[865] The case concerned an employee of the Prince of Wales who supplied certain copies of his private journals to newspapers, which expressly violated the confidentiality clause within the employee's terms of employment.[866] The journals reflected (amongst other things) Prince Charles' personal feelings about his royal tours and other issues connected to his duties, such as the handover of Hong Kong from the UK to China. However, the journals were not solely for the Prince's personal use – there was a list of recipients to the journals:

> 'the journals were not created merely for personal contemplation by the claimant but were created for the purpose of circulation with the intention of affecting others' opinions. They were circulated to at least 50 to 75 persons, including politicians.'[867]

The judge ultimately held that, regardless of the (relatively small) amount of people the Hong Kong journal had been sent to, the information was not already in the public domain and that the Prince had intended his journals to remain confidential.[868] The defendant publishers (a large newspaper corporation) sought to argue that the fact that the Prince was lobbying democratically elected ministers was of public interest – as heir to the throne, he was expected to be politically neutral.[869] The judge ultimately held that the articles in question did not discuss lobbying – with one exception – and so a public interest in respect of this was not generated.[870] The judge concluded that the Prince of Wales' privacy overrode any countervailing Article 10 interest of the journals or newspaper articles which concerned them:

> 'Not the least of the considerations that must be weighed in the scales is the claimant's countervailing claim to what was described in argument as his private space: the right to be able to commit his private thoughts to writing and keep them private, the more so as he is inescapably a public figure who is subject to constant and

[864] Jon Silverman, 'Ruling puts pressure on celebrity books' (*BBC News*, 14 December 2006), accessible at: http://news.bbc.co.uk/1/hi/entertainment/6181333.stm (last accessed 8/8/19).
[865] [2006] All ER (D) 335.
[866] Ibid [2-9].
[867] Ibid [64].
[868] Ibid [100-2].
[869] Ibid [123-4].
[870] Ibid [129].

> intense media interest. The fact that the contents of the Hong Kong journal are not at the most intimate end of the privacy spectrum does not, to my mind, lessen the force of this countervailing claim'.[871]

In essence, the Court found here that protecting the Prince's private space was of paramount concern. Two years after this decision and that in *McKennitt* came the judgment handed down in *Mosley v MGN*. Here, the High Court found that, again, the privacy rights of a private individual won out against a news corporation. In the case, Max Mosley succeeded in winning damages against the News of the World for publishing details about his sadomasochistic encounters with sex-workers. Mosley was found to have a reasonable expectation of privacy – particularly because of the intimate nature of the activities involved. Mr Justice Eady noted in his judgment:

> '…is not for the state or for the media to expose sexual conduct which does not involve any significant breach of the criminal law. That is so whether the motive for such intrusion is merely prurience or a moral crusade. It is not for journalists to undermine human rights, or for judges to refuse to enforce them, merely on grounds of taste or moral disapproval.'[872]

Mosley was awarded a not insubstantial amount of money for a privacy claimant in £60,000[873] as the court found that there was not a legitimate public interest argument that could override Moseley's privacy rights in the case. Central to the decision, Mr Justice Eady found that the paper's public interest argument *did not outweigh* Mosley's reasonable expectation of privacy – particularly as, on the facts, the papers could not prove that the orgy in question had a Nazi theme or element to it.[874] Mr Justice Eady noted that in deciding early cases in MPI after *Campbell*, 'broad generalisations' in judgments must be avoided – for example, the assumption that because someone is a celebrity that they do not have a right to privacy.[875] In his finding, Mr Justice Eady relied heavily upon the abovementioned decisions

[871] Ibid [133].
[872] *Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB) [127].
[873] For a discussion on monetary awards in MPI cases, see the section below in this chapter on remedies.
[874] Mosley above n 872 at [24-72], [97], [108] and [123].
[875] Ibid at [12].

of *Campbell* and *Von Hannover*.[876] Although Mosley received substantial damages in the case, he did not succeed in obtaining an interim injunction (as the information was already in the public domain)[877] and the decision ultimately did not aid Mosley in deleting videos taken of the orgy online.[878]

No one can doubt the significant impact that these cases in particular have had on the development of MPI in English law - particularly the decision of the House of Lords in *Campbell.* Thanks to this, claimants now do not have to prove that they have disclosed information within a confidential relationship in order to succeed in their claim. However, the trajectory of MPI case law has not been exclusively positive, from a privacy advocate's (or a claimant's) perspective. In a move away from the robust protection of privacy rights that the above cases advocate, some later High Court decisions of the English courts have shown a tendency to accept weak public interest arguments and prioritise these over the legitimate privacy rights of claimants. Due to this, the approaches of the judiciary to the balancing exercise in MPI judgments can be described as erratic or inconsistent. These decisions will now be discussed in detail.

Notable examples of the prioritisation of flimsy public interest arguments on the parts of the court are present in the cases of *Ferdinand* and *Terry*.[879] Both of these cases have been discussed at length in chapter 4 of this thesis, which concentrates on the conception of the public interest (and its various 'sub-factors'). Here it suffices briefly to recall that in both cases the court accepted that the tenuous notion of the 'role model' factor legitimised the publication of details of both John Terry and Rio Ferdinand's extra-marital affairs.[880] The courts agreed with defence counsel that as Terry and Ferdinand had young fans this information therefore had public interest value, despite the fact that neither had engaged in illegal conduct or behaviour that affected the public at large in any way.[881] The notion of the 'right to criticise' was also invoked and accepted by the Court in *Terry*: it finds that theoretically *any* private information can be published, as it is important to encourage societal

[876] Ibid at [11-22].
[877] See below for a section on the 'public domain' in MPI caselaw.
[878] The author herself was able to access a video of Mosley and the sex-workers as late as 2014-2015 through a simple Google search.
[879] *Terry* and *Ferdinand*.
[880] *Ferdinand* [87].
[881] As is elaborated upon in chapter 4.

critique and debate.[882] As has been stated in chapter 4 this argument covers a potentially unlimited array of personal information, and also lacks a sound legal principle; it is not necessary to disclose private facts about an individual's life in order to encourage discussion about living habits and behaviours, as this can be done through various forms of expression.[883]

As stated above, in their acceptance of feeble public interest arguments, the English judiciary here relied upon their own conceptions of morality in order to find that there was a legitimate public interest in the private lives of celebrities, despite the fact that the cases concerned mundane and banal information.[884] The judicial acceptance of the role model argument demonstrates this well – the argument legitimises the publication of *moral* wrongdoing, and the exposure of it. In *Terry*, Mr Justice Tugendhat implied that discouraging immoral behaviour is a valid justification for finding that a piece has public interest value.[885] Mead has also observed that various different *private* interests (such as a lascivious interest in the sex lives of the famous) are bundled into judicial decisions concerning what constitutes the *public* interest.[886] This is particularly evident in these two cases.[887] The approach of the court in this regard can be contrasted with the method that Fenwick and Phillipson advocate regarding MPI claims: that only *genuine* arguments of important public interest should be tolerated and accepted by the courts, in order to ensure the protection of Article 8 rights.[888] By accepting flimsy public interest claims, the courts in *Ferdinand* and *Terry* failed to properly assess the value of a competing free speech interest on the part of a defendant publication. The notion of public interest was therefore stretched to encompass low-level speech,[889] including gossip mongering.[890] In doing this, the courts failed to conduct a genuine parallel analysis, as stretching the notion of public interest in this way indirectly prioritises Article 10 rights over Article 8 – as even weak public interest claims were held to trump a reasonable expectation of privacy. Other academics such as Wragg, however, argue that assessing the value of a

[882] *Terry* [104] (Tugendhat J).
[883] Phillipson and Fenwick above, n 819 at 690.
[884] An example of important speech being that which is political or artistic.
[885] Paul Wragg, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) *Journal of Media Law* 225, n 839 at 236 and *Terry* [104].
[886] David Mead, 'A socialised conceptualisation of individual privacy: a theoretical and empirical study of the notion of the "public" in MoPI cases' (2017) 9(1) *Journal of Media Law* 100, 130.
[887] Ibid.
[888] Phillipson and Fenwick above, n 819 at 690. C/f Wragg above, n 839 at 237.
[889] In other words, that which does not meaningfully relate to one of freedom of expression's core theoretical rationales: the pursuit of important truths, the facilitation of democracy and personal autonomy. See Chapter 4.
[890] As was argued in chapter 4 of this thesis concerning Article 10.

public interest claim through *scrutinising the quality of the speech itself* is unprincipled.[891] A strong objection is levelled here against his argument: conversely, this is the *most* principled way of conducting the balancing exercise in a legitimate fashion. By conducting a thorough examination of the quality of the speech at stake, the courts can meaningfully gauge whether the public ought to know the private information (which would be the case if, for example, it exposed the wrongdoing of someone in public office which directly affects citizens) or whether the data has little public interest value but significant value in terms of a claimant's privacy (which would likely be the case in the event that it is particularly intimate).

Wragg does not explain why the value of a speech interest in an MPI claim should not be robustly assessed. Both Article 8 and 10 rights are considered equal under the ECHR, and the English case of *PJS* has recently confirmed that section 12 of the Human Rights Act (which urges the courts to take into account the effect of their judgments on freedom of expression) does not mean that Article 10 rights automatically outweigh Article 8 interests in MPI cases.[892] Not all speech is of equal value – important political speech, even if it relates to an individual's private life, deserves utmost Article 10 protection.[893]But it is crucial that valuable speech is contrasted with imprecise claims about disclosures linked to a person's private life that have no meaningful societal impact. Indeed, this was done by Lord Hoffmann in *Campbell*, who stated that the 'relatively *anodyne nature* of the additional details is in my opinion important and distinguishes this case from cases in which (for example) there is a public interest…'[894] It is argued here that the information in both *Ferdinand* and *Terry* falls into this category of anodyne speech. The lack of a meaningful assessment of the importance of speech in both cases directly led to the courts' mischaracterisation of the public interest.

While *Terry* and *Ferdinand* occurred in 2010 and 2011 respectively (both after the abovementioned cases of *Campbell*, *McKennitt*, *Prince of Wales* and *Mosley*), there is some evidence to suggest that the tide has now turned back again to fairly balancing Article 10 and Article 8 rights due to the judgment of the Supreme Court in *PJS* in 2016.[895] In the case, which concerned the sex life of one half of a celebrity couple,[896] Lord Mance stressed the importance of judicial consideration of the value of speech in MPI cases and opined that low-

[891] Wragg above, n 839.
[892] *PJS* [19 and 20].
[893] See for example *Plon (Societe) v France* App no 58148/00 (ECHR, 18 May 2004).
[894] *Campbell* [60].
[895] *PJS*.
[896] The case will be discussed in more detail later in this chapter.

level tittle-tattle about the private lives of celebrities may not be protected under Article 10. When considering upholding an injunction barring the publication of details concerning the celebrity's extra-marital affairs, he stated:

> 'But, accepting that Article 10 is not only engaged but capable in principle of protecting any form of expression, this type …is at the bottom end of the spectrum of importance…'[897]

He went on to hold that information about sex lives often lacks legitimate expression value:

> 'In these circumstances, it may be that the mere reporting of sexual encounters of someone like the appellant, however well known to the public, with a view to criticising them *does not even fall within the concept of freedom of expression under Article 10 at all*…'[898]

This particular observation is of interest when contrasted with the approach of the courts in *Ferdinand* and *Terry,* both cases concerning the sex lives of professional footballers. It is clear from the above quotations that the approach of the Court in *PJS* is different to that in *Ferdinand* and *Terry*. This trend continued in the 2018 case of *Sir Cliff Richard*,[899] in which Mr Justice Mann considered the notion of public interest at length. In assessing whether the disclosure that Sir Cliff Richard was being investigated for historical sexual abuse had legitimate public interest value, the judge noted that a point of relevance was the motive of the BBC in making the disclosure.[900] He observed that 'I think that they, or most of them, were…impressed by the size of the story and that they had the opportunity to scoop their rivals'[901] and that although the matter did invoke aspects of the public interest,[902] this monetary-led motivation counted against the BBC's case.[903] The judge ultimately held that naming Sir Cliff Richard as subject of the investigation *did not* have legitimate public interest value despite the fact that it 'might be of interest to gossip-mongers' as Sir Cliff had not been

[897] *PJS* [24].
[898] *PJS* [24 - emphasis added].
[899] *Sir Cliff Richard*.
[900] *Sir Cliff Richard* [279-280].
[901] *Sir Cliff Richard* [280].
[902] For example, the reportage of crime would generate a legitimate public interest – but here Sir Cliff had not been charged and ultimately, never was (see [312] in the judgment).
[903] *Sir Cliff Richard OBE*) [280-282.]

charged.[904] It can be said that Mr Justice Mann here analysed in detail the breadth of speech that can be considered to be in the public interest as well as its relative value.

The recent decision of *Sir Cliff Richard* is reminiscent of the judgment in *PJS* in more ways than one. *PJS* considered in detail the level of intrusion for the claimant and his family in the case if publication were to be allowed, this factor significantly contributing to the award of an interim injunction.[905] Similarly, a key consideration in *Sir Cliff Richard* was the level of intrusion that Sir Cliff had had to suffer from the media after the BBC had named him in conjunction with the police investigation, and the negative impact this was having on his life. The judge observed:

> 'Sir Cliff felt trapped in his own home, and he felt despair and hopelessness leading, at times, to physical collapse. At first he did not see how he could face his friends and family, or even his future.'[906]

A large part of the judgment is dedicated to extensive reports on the BBC concerning the police investigation into Sir Cliff; the BBC reported the issue on its television networks ten times within two days, giving updates as to the police activity in Sir Cliff's home and whether they had taken any objects as evidence.[907] This was alongside subsequent reports on other service stations, publications online[908] and newspaper coverage that followed the BBC breaking the story. Mr Justice Mann used the level of press intrusion into Sir Cliff's private life to justify the balancing act as tipping in Sir Cliff's favour, with his Article 8 rights prevailing as opposed to the public interest 'defence' the BBC attempted to argue.[909] The restatement of the importance of claimants' rights and the emphasis on a robust assessment of genuinely important speech in the two cases of *PJS* and *Sir Cliff Richard* is a welcome development – especially as *PJS* is a judgment from England and Wales' most senior court, being arguably the most important case in this area since *Campbell*.

[904] And the presumption of innocence must be upheld. See *Sir Cliff Richard* [282] and [316-7].
[905] See *PJS* [29]. The role of 'intrusion' on private life as a factor in *PJS* will be discussed in more detail later in this chapter. Interim injunctions will also be discussed in the 'Remedies' section of this chapter.
[906] *Sir Cliff Richard* [233].
[907] *Sir Cliff Richard* [117-142].
[908] See *Sir Cliff Richard* [147]: the BBC's own online article relating to the story garnered 5.1 million hits.
[909] *Sir Cliff Richard* [317].

Conclusion

Although the jurisprudence in this field is complex and contradictory, *PJS* will have a major influence on future judgments, and such influence is already apparent in the *Cliff Richard* cases. *PJS* has addressed the criticism that the public interest has been interpreted too expansively in prior caselaw, *to an extent*. Criticism of the tort in this regard is therefore less pertinent than in some other areas, except in respect of the public interest arguments that were not specifically mentioned in the case – such as the role model[910] and press-as-a-watchdog arguments (discussed at length in chapter 4). In respect of these public interest arguments, lower courts might view themselves as still having leeway to take an expansive approach. There also remains the possibility that future caselaw tenuously distinguishes itself from the judgment in *PJS*, in a move to take a differing stance. This would not be entirely unusual for privacy caselaw: it could be said that the pattern of cases has wavered from *restrictive-expansive-restrictive-expansive* approaches to privacy rights since the 1980s and this latest expansive trend is just temporary.[911]

What has been concluded by the prior section of this chapter is that the courts' approach to the balancing act conducted in MPI between privacy has been erratic. After a slew of caselaw which arguably, balanced privacy and expression rights genuinely and fairly (*Campbell*, *McKennitt*, *Prince Charles* and *Mosley*), the High Court delivered two judgments which went against this grain and accepted an extremely broad interpretation of the public interest, prioritising press freedom. Erratic judgments on the part of the English courts in this regard are an endemic weakness of the tort. Neither decision of *Terry* nor *Ferdinand* has been formally denounced by the English courts (with one exception of one factor utilised in *Terry* – the right to criticise as per Lord Mance in *PJS*),[912] leading one to believe that both judgments are still good law. This is despite the fact that they both sit uncomfortably alongside some earlier cases such as *Campbell*.[913] What this divergence serves to show is that MPI is a fickle friend to claimants – even with what appears to be a 'strong case', it is ultimately unclear up to trial which side of the balance judges will err on – and how

[910] Although it could be argued that the courts *impliedly* distanced themselves from this factor – as they did not hold that the celebrity status of the couple (the claimant's husband in particular) barred an injunction in the case.
[911] Initially, prior to the Human Rights Act, the English courts were reluctant to recognise a right to privacy in English law, this most evident in the case of *Wainwright* above, n 820 [28-35]. This restrictive trend ceased in the famous case of *Campbell*, but it could be argued once again returned within the judgments of *Ferdinand* and *Terry*. Perhaps the tide has turned once again in favour of privacy in *PJS* and *Sir Cliff Richard* – but for how long remains to be seen.
[912] See chapter 4 of this thesis – 'recent developments in the right to criticise'.
[913] Which also has superior precedent, as a House of Lords decision.

significant a public interest argument has to be in order to persuade judges to uphold publication, or Article 10 rights.

This weakness is problematic not only for private information disclosed offline but also (in the context of this thesis) online publication: this bias could impact the use of the tort in respect of a data subject wishing to take an action in MPI regarding information disclosed (or about to be disclosed) on the web.[914] However, it is important to note that in certain circumstances, a person would be able to utilise MPI in order to obtain an injunction against information disclosed about themselves online, and in the case of an ordinary individual, specific balancing exercises relating to celebrities would be irrelevant. However, further flaws of MPI as will be discussed below indicate that MPI's ability to constrain information posted to the internet is limited.

It must be noted that the introduction of the right to be forgotten gives the English judiciary somewhat of a 'new start' with regards to privacy and expression balancing. It is difficult to predict at this stage whether the English courts will once again ricochet in their judgments between fairly balancing privacy and expression interests and unfairly prioritising expression with regards to Article 17 claims – this is indeed an unfortunate possibility. It is encouraged here that the English courts should learn from their prior mistakes with regards to the poor balancing exercises conducted in the cases of *Terry* and *Ferdinand* and not fall into a similar pitfall with regards to the new erasure right in the future. Indeed, the court's recent judgments in *PJS* and *Sir Cliff Richard* do provide some relief for privacy advocates.

D. The various interpretations of the doctrine of waiver in MPI

In a handful of cases from the 1970s on[915] in breach of confidence and MPI, English courts have created a doctrine of implied 'waiver' of privacy rights. The doctrine assumes that an individual can negate their right to privacy through their own previous solicitation of publicity. The Press Complaints Commission applies something similar; a 2012 report concerning press reportage annexed to the Leveson Inquiry stated that:

[914] See for example *AMP v Persons Unknown* [2011] EWHC 3454 (TCC).
[915] For example, see *Woodward v Hutchins* [1977] 2 All ER 751, [1977] 1 WLR 760.

> '…Editors will be expected to justify intrusions into an individual's private life without consent. *Account will be taken of the complainant's own public disclosures of information*.'[916]

Some academics have (rightly) expressed concern over the doctrine, protesting that it is not 'plausible'.[917] The fact that a person has disclosed *certain private facts* about themselves publicly should not accord the press 'carte blanche' to disclose *other* pieces of private information about them in the future.[918] The doctrine can therefore be seen as unjustly interfering with an individual's informational control and personal autonomy.[919] In addition to these concerns, the English courts' principle of waiver has not been consistently defined. Long before the inception of the Human Rights Act, a broad notion of waiver had been embraced – this being that if a celebrity had *on any occasion* courted press attention, then they should be seen as having abandoned any interest in keeping their personal life private.[920] Lord Bridge stated in *Hutchins* (1977):

> 'those who seek and welcome publicity of every kind bearing upon their private lives so long as it shows them in a favourable light are in *no position to complain* of an invasion of their privacy…'[921]

Later cases have moved away from this approach – not coincidentally, but to accord with the judicial obligation of courts under the Human Rights Act 1998 to act compatibly with ECHR rights, including Article 8.[922] *Douglas II* in 2003 found that a person's prior solicitation of publicity would not have *general* relevance; rather, what would be important would be how the complainant had acted in respect of the information *in question*.[923] This is a much narrower conception of waiver than that advocated in *Hutchins*, as it relates to disclosure of the specific information in question. *A v B* two years later suggested an alternative approach:

---

[916] Excerpt taken from a timeline of the Press Complaints Commission's Code of Practice (guidelines) since 1991. See 'Press Regulation in the UK: summary' (*National Archives*, Leveson Inquiry 2012) available at: http://webarchive.nationalarchives.gov.uk/20140122191640/http://www.levesoninquiry.org.uk/wp-content/uploads/2012/07/DCMS-submission_Narrative-on-press-regulation.pdf (last accessed 12/6/18) 23.
[917] See Phillipson and Fenwick above, n 819 at 680.
[918] Ibid.
[919] Phillipson and Fenwick above, n 819 at 680.
[920] *Woodward v. Hutchins* [1977] WLR 760.
[921] Ibid [emphasis added].
[922] The Human Rights Act 1998, section 6.
[923] The information that is subject to the breach of confidence or misuse claims. *Douglas v Hello! Ltd* (*No.2*) [2003] EWCA Civ 139; [2003] EMLR 585 [226].

the notion of zonal waiver.[924] A key consideration of the courts, it was found, in assessing waiver was the *type* of information a data subject had previously disclosed.[925] If it was the same type (or, as the name suggests, in the same 'zone') as information that a defendant publication wished to or had[926] disclosed, then the claimant's reasonable expectation of privacy could be seen as being waived.[927] This approach is broader than *Douglas II*'s interpretation, in the sense that an informational zone has the potential to be large, depending upon what had previously been disclosed. Regardless of this problem with zonal waiver, it undoubtedly covers a narrower area than that advocated by *Hutchins*. *Sir Cliff Richard* considered the notion of zone-based waiver in relation to Sir Cliff Richard's extensive fame and charity work, Mr Justice Mann stating that '[the] very act of making certain aspects of oneself public means, by definition and by logic, that there is a corresponding loss of privacy in those areas which are made public. However, it does not follow that there is some sort of across the board diminution of the effect of privacy rights'.[928] The judge adopted a narrow conception of zonal waiver, stating that it would only be legitimate to expose Sir Cliff as doing 'un-Christian' things, and that an *allegation* made against him of sex abuse did not fall into this category.[929] Overall, Mr Justice Mann attached little importance to the notion of Sir Cliff waiving his privacy rights in respect of his celebrity status, stating that the fact he was well known made his privacy rights more, rather than less, pertinent.

Adding further uncertainty into the usage of this concept, even though the claimant and his famous partner had spoken to the press about their family life (in the past) in *PJS*, this did not prohibit an injunction being awarded in the case.[930] Arguably, zonal waiver could have been referred to and utilised in *PJS* as the couple in question had, in the past, spoken about having an 'open marriage' – however, waiver was not discussed in the Supreme Court's judgment. It is also important to note that in the most seminal decision of MPI thus far, *Campbell*, the notion of waiver did not feature in the judgment. Generating even more confusion, there has also been a recent case that suggests that there is the potential for a claimant's privacy to be waived by someone else. In *AAA v Associated Newspapers* the claimant was the lovechild of

[924] [2005] EMLR 36.
[925] *A v B* [2005] EMLR 36 [21-28].
[926] *Ex post facto*, had disclosed, in an action for damages.
[927] *A v B* [2005] EMLR 36 [28].
[928] *Sir Cliff Richard OBE* [284].
[929] *Sir Cliff Richard* [285].
[930] *PJS*.

a famous politician; the article in question discussed the claimant's paternity.[931] It was held at first instance (and confirmed on appeal) that the claimant's reasonable expectation of privacy was reduced because of comments her *mother* had made about her private life and her daughter's parentage to a director of a magazine at a party and an interview her mother had given.[932]

The doctrine of waiver is problematic for several reasons. Firstly, it is unjust to say that because a person has chosen to disclose *one* piece of information about a particular aspect of their private life in the past that they have relinquished control over other pieces of private information about themselves. Far from it: it is more logical that autonomy and control over the remaining information should be maintained as they have specifically chosen *not* to disclose it.[933] As discussed, that provides one reason for the courts' rejection under the Human Rights Act of the general waiver argument. Regarding zonal waiver, there may be particular reasons why a person is happy to disclose a certain fact about an aspect of their personal lives but not another fact, still within this zone. By way of illustration, a person may be happy to disclose that they are in a relationship but not want any details about who they are in a relationship *with* to become available: to a celebrity, this might be particularly important. A person in the public eye may be happy to give a limited amount of information away, but not enough that their private life is intruded upon – if too much detail about their love life is given this could lead to their partner being harassed by the media. Due to the complex and incoherent nature of the caselaw on zonal waiver, it is not definitively clear whether a zonal waiver model would legitimise the disclosure of who a celebrity was dating in the above example. However, it could be one interpretation given the reasoning in *A v B*, where the court held that further publication by a third party of a rock-star's drug abuse was legitimate, because he had chosen to discuss some aspects of his drug-taking in other interviews in the past. The court stated:

> 'in identifying the scope of material within the public domain, once such a claimant has chosen to lift the veil on his personal affairs, the test will be "zonal"; that is to say, the court's characterisation of what is truly in the public domain will not be tied specifically to the details revealed in the past *but rather focus upon the general area or zone of the*

[931] *AAA v Associated Newspapers* [2013] *AAA v Associated Newspapers Ltd* Court of Appeal (Civil Division), [2013] EWCA Civ 554.
[932] Ibid.
[933] Waiver arguments and the Strasbourg court's approach is discussed in chapters 3 and 4 of this thesis.

claimant's personal life (e.g. drug addiction) which he has chosen to expose.'[934]

Therefore, the zone of disclosure about his previous drug abuse was 'fair game' – even in respect of previously undisclosed facts.[935] Counsel could endeavour to draw parallels between the prior disclosures of drug-taking and information about a relationship in the above example. This distinction between data as voluntarily provided and that which remains undisclosed is a fundamental facet of an individual's informational autonomy. Rowbottom has stressed the importance of this, stating that 'people should have the right to negotiate their public profile…and contextualise information.'[936] Removing informational autonomy from a data subject in this way is undoubtedly damaging. Auburn has noted that this type of 'confidentiality-based' waiver is not an argument that is rooted in 'fairness'; rather it is a condition imposed upon a right existing.[937]

Consideration must be given to zonal waiver and the eventuality that a person needs to disclose personal data in order to refute allegations or 'challenge claims.'[938] An example of this in recent history concerns Princess Diana who opted to give interviews to certain news outlets after her divorce from Prince Charles, exposing her feelings about her treatment by the British royal family.[939] If a person's actions in coming forward and discussing certain topics are to be seen as waiving their right to privacy in respect of a large zone of their personal information, this may have the damaging impact of actively discouraging individuals from defending themselves against unfair claims. It also encourages self-censorship, even in the event that a person has not engaged in any wrong-doing. As argued above, what constitutes a zone has the potential to be extremely broad. If a person's political persuasions can be seen as a zone, then this would obviously encompass whom they voted for in the last general election but could also include their views about marriage or any other part of their life which is governed by politics. This issue was considered in the case of *The*

[934] *A v B, C and D* above, n 847 at [28].
[935] Ibid.
[936] Rowbottom above, n 817 at 182.
[937] Jonathan Auburn, 'Implied Waiver and Adverse Inferences' (1999) 115 *Law Quarterly Review,* 590, 593.
[938] Rowbottom above, n 817 at 182.
[939] See for example, Cecila Rodriguez, 'Princess Diana: Three New Documentaries Reveal More Secrets, 20 Years After Her Death' (*Forbes*, 28 July 2017) accessible at: https://www.forbes.com/sites/ceciliarodriguez/2017/07/28/princess-diana-20-years-after-her-death-three-new-documentaries-reveal-more-secrets/#138191fa1c4a (last accessed 13/7/18).

Prince of Wales which considered a breach of confidence claim - a distinction was drawn between the Prince's public speeches and more private writings.[940]

The digital era could also be seen to have shifted the boundaries of what a court should deem an informational zone to be. It is likely that the majority of people in England and Wales have *some* aspect of private information available about themselves currently online, from electoral roll details to photographs of themselves and loved ones on Facebook.[941] If a person has, for example, one photograph of themselves and their partner openly accessible on a social media site, according to the zonal argument does this mean that other private aspects of their relationship can be routinely disclosed without consent? This may appear unlikely, but it cannot be doubted that this area of the jurisprudence lacks clarity; the outer limits of what constitutes zonal waiver are left undefined. The doctrine appears to be incompatible with the commonplace disclosure of 'sharing privately' online.[942]

In relation to the above-mentioned data dissemination scenarios, regarding the *personal public disclosure scenario*[943] a person would fail to have a reasonable expectation of privacy in respect of this information, according to MPI under the zonal waiver doctrine. Aside from this, the notion of waiver would further bar any claim for a subject in the tort, as their initial act of uploading would again probably negate an action. The same could also be said of the *third party poster* scenario,[944] as if the courts took heed of *AAA v Associated Newspapers* then a third party uploading personal data about another online could be seen as akin to the mother in the case disclosing private information about her child, waiving her child's privacy rights.[945] If the third party here was not seen as *de facto* waiving the data subject's rights, then an MPI claim could potentially fail on the basis that the information was already in the public domain regardless of who uploaded it.[946]

---

[940] *HRH The Prince of Wales v Associated Newspaper*s (*No.3*) [2006] EWCA Civ 1776; [2008] Ch 57; [2007] 3 WLR 222; [2007] 2 All ER 139; [2008] EMLR 121; The Times, 28 Dec 2006 [88].

[941] There is a 'free' electoral roll search which gives names and addresses (as well as those of co-occupiers) openly accessible on the internet on website *192.com*, accessible at: https://www.192.com/people/electoral-roll/ (last accessed 13/7/18). Reportedly 83% of adults in the UK now have one or more social media accounts: see (*Avocado Social*, 2 April 2018) accessible at: https://www.avocadosocial.com/the-latest-uk-social-media-statistics-for-2018/ (last accessed 13/7/18).

[942] See Max Mills, 'Sharing privately: the effect publication on social media has on expectations of privacy' (2017) 9(1) *Journal of Media Law* 45.

[943] Where a data subject has initially uploaded personal data about themselves to the Internet and subsequently wishes to remove it.

[944] Where a third party uploads the personal data of another and that person wishes to remove it.

[945] *AAA* above, n 931.

[946] This will be discussed in detail in the section below.

To sum up, the notion of waiver could present a problem for someone seeking to rely on MPI in respect for information that has already (or is about to be) disclosed about them online. Waiver as a concept can apply to ordinary persons but it is less likely to do so – as they are less likely to have, for example, given interviews to on or off-line media bodies. However, in the context of this thesis' data leak scenarios, person X may have posted some personal data online by relaxing a part of their privacy settings on a social network (at a particular time) – and this could be then posted elsewhere by third parties (the *restricted access* scenario). Using the arguments made out by the courts in waiver, the doctrine could potentially apply in this scenario if X sought to obtain an injunction in MPI to require that the material is deleted and no longer disseminated. Privacy advocates would argue that it should not, as X has taken steps to protect their privacy – however, many broad readings of waiver have been demonstrated in the caselaw discussed above. In a circumstance where a data subject has their social media account set to public access *all of the time*, and then a photograph is reposted elsewhere (to the distress of the subject) it would be easy to adduce a waiver argument that they had negated their right to mount a successful claim in MPI, as no steps had been taken to stop dissemination of this information (the *personal public disclosure* scenario). The *possibility* that waiver could apply in this circumstance adversely affects the potential of MPI to protect online privacy, despite the fact its application in the caselaw has been patchwork.

Conclusion

In light of the arguments outlined above, this section has attempted to show that waiver as a concept is harmful to the rights of claimants in MPI, irrespective of the new deletion right. It is an archaic concept that has been (at times) broadly drawn and personality rights under Article 8 have suffered. Although its application has been intermittent, the concept also does collective harm: robust privacy rights support society, as aspects of privacy support sociality.[947] This uncertainty in the law does nothing to help privacy claimants. This chapter will now turn to the third reason why MPI as a tort is, it will be argued, ineffective at securing online personality rights – the notion of information as 'already in the public domain'.

[947] Mead above, n 886 at 129.

E. The notion of information already in the 'public domain'

This concept within MPI is related to the requirement within breach of confidence that the information is *confidential in nature*.[948] It provides that if the private information is deemed to already be in the public domain then it is less likely that the courts will find that a reasonable expectation of privacy exists, cautious about encroaching upon Article 10 interests.[949] A MPI claim may therefore fail. Section 12(4) of the Human Rights Act has also influenced this concept – section 12(4) states that the courts must 'have regard to the extent to which the information has become, or is about to become, available to the public'[950] when considering awarding an injunction. However, MPI is not solely concerned with protecting 'secrets' which no one other than the claimant knows: there are limits to the public domain doctrine, as caselaw has shown that the tort claim can still be successful if a limited amount (or even a large number) of people are aware of the private information.[951] It is unclear where the line is drawn by the courts with regards to *how public* information has to be to invoke this doctrine. It should be noted that in the cases of *Campbell* as well as *Peck* and *Von Hannover* at the ECtHR a number of people were in the street at the time the photographs[952] in each case were taken (in the case of *Von Hannover*, a number of people in a restaurant and beach club) and therefore could have witnessed the information in question. Despite this doctrine, the information in all cases was still deemed 'private'. Similarly, in the case of *Mosley* a very large amount of people already knew of the information as it had been reported in the newspaper; although the claimant still 'won' his case, his remedy was negatively affected as a result.[953] This serves to show that even where data is to an extent public knowledge that it is not necessarily capable of unilaterally defeating a claim - other factors can tip the balance. In *Von Hannover*, Princess Caroline was surrounded by a climate of 'continual harassment' that strengthened her Article 8 claim. Naomi Campbell was seeking treatment for substance abuse which bolstered her claim in her case due to the sensitivity of the subject matter – similarly,

[948] Deakin, Johnson and Markesinis above, n 821 at 845.
[949] Ibid at 845.
[950] Human Rights Act 1998.
[951] *CTB v News Group Newspapers Limited* 2011] E.W.H.C. 1326 QB. [23] (Eady J) as referenced by: Mo above, n 837 at 94. In both the abovementioned cases of *Terry* and *Ferdinand*, both claimants were found to have a reasonable expectation of privacy despite the fact they had disclosed their affairs to selected people and, in the case of *Terry*, rumours were circulating – the information could not be said to legitimately be within the public domain.
[952] More specifically, in Peck's case, CCTV footage which stills were obtained from. See *Peck v United Kingdom* App no 44647/98 (ECHR, 28 January 2003).
[953] Mosley's injunction was not maintained. See *Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB).

the images and CCTV footage of Mr Peck that were the subject of his claim depicted his suicide attempt, again warranting a higher degree of protection.[954]

Indeed, Wragg argues that MPI claims can survive some element of 'public disclosure' unlike breach of confidence claims,[955] and Hughes has observed that information already in the public domain but of a *particularly intimate nature* (in one case, a sex tape) can still attract liability in MPI.[956] *Spycatcher* expounded that if information has only been disclosed to a *limited* part of the public, it will not be within the public domain.[957] The issue that remains is what constitutes 'limited'. In the recent case of *Reachlocal* which specifically concerned online information, it was held that 'tweets' on Twitter viewed by a few thousand could be considered to be in the public domain.[958] In comparison, the Northern Irish case of *Martin and Ors* found that publication to a private Facebook account (where viewers were controlled) did not count as placing the information in the public domain.[959]The difficult situation must also be considered whereby a person initially posts something to a private Facebook account, as in *Martin and Ors*, but it is then reposted to a public part of the internet by a third party (the *restricted access* scenario). This question was raised in *Rocknroll v NGN*: here the case was decided in favour of the claimant, on the grounds that there was in fact something private left to protect – the act of reposting the information to a more public platform could engender greater harm to his reputation.[960] It is interesting to compare the case in *Rocknroll* to the more traditional judgments of *Terry*, *The Prince of Wales* and *A v B.*[961] In all of these cases, the argument was run that there was something private left to protect, potentially warranting damages or an injunction against the information's disclosure, although in two of those instances a remedy was denied on other grounds. Only a limited amount of people knew about the love affairs in *Terry* and *A v B* and not many people had access to the Prince's personal writings in *The Prince of Wales.*[962] This approach can be

[954] *Von Hannover* [68], *Campbell* [461] and *Peck* above, n 952 [10].
[955] Paul Wragg, 'Privacy and the emergent intrusion doctrine' (2017) 9(1) *Journal of Media Law* 14, 16. Also see *PJS* [18].
[956] See Kirsty Hughes, 'Publishing Photographs Without Consent' (2014) 6(2) *Journal of Media Law* 180 and *Contostavlos v Mendahun* [2012] EWHC 850.
[957] *Attorney General v Guardian Newspapers Ltd* (No2) (1991) 14 EHRR 229 [54-55].
[958] *Reachlocal UK Ltd v Bennett and Ors and Mason v Huddersfield Giants Ltd* [2013] EWHC 2869 (QB).
[959] *Robert Gordon Martin and Heather Elaine Martin and Ors v Gabrielle Giambrone P/A Giambrone & Law, Solicitors and European Lawyers* [2013] NIQB 48.
[960] *Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch) [25].
[961] *Terry, HRH Prince of Wales v Associated Newspapers* [2006] EWCA Civ 1776 and *A v B* [2002] EWCA Civ 337; [2003] QB 195; [2002] EMLR 371; [2002] 3 WLR 542; [2002] 2 All ER 545. *A v B* concerned a footballer's affair with a lap-dancer and another woman.
[962] Ibid.

contrasted to that in *Theakston* – photographs of the claimant in a brothel were deemed not to be confidential as '[it] is likely that other customers and a number of prostitutes will see who comes and goes'.[963] *Theakston* may well have been decided the way it was because the judiciary, in importing issues of sexual morality into their judgment, came to the conclusion that Theakston as engaging in these activities ran a risk of his proclivities being exposed.[964] Regardless of why the case was decided in that manner, the judgment in *Theakston* is out-of-date and clearly does not comfortably align with subsequent caselaw.

As the above analysis has demonstrated, the traditional test to establish whether the information is already in the public domain is whether there is *anything private left to protect*. Mills has suggested that in order to utilise the doctrine in the digital age, it would be better to instead consider the *intentions of the original poster* in uploading information about themselves. Indeed, the 'intention to abandon confidentiality' is a rehearsed argument in favour of finding that privacy rights have been waived.[965] Some considerations under this new test could include whether a person intended their data to be available for viewing to a limited number of approved individuals on social media (the *restricted access* scenario) rather than publication to a much wider audience.[966] This is linked to 'foreseeability' considerations: in other words, whether it was foreseeable that the data would be broadcast to a large number of people.[967] Under this analysis a person would not be responsible if their post was disseminated to a larger audience through third party intervention, and their MPI action could succeed. However, this test has its limitations: it may not allow for a remedy to be found in MPI for data dissemination where a data subject has initially uploaded the personal data online themselves to a public platform, the data subsequently being reposted by others and leaving their control.[968] Their initial intention at the time of posting was presumably to make the information somewhat public. The GDPR, and in particular Article 17, has been designed to allow a data subject to change their mind and subsequently revoke consent to processing – unfortunately, Mills' new formulation of the public domain test fails

[963] *Theakston v MGN* [2002] EMLR [62].
[964] A similar argument was made by the judiciary in the cases of both *Ferdinand* and *Terry*; the thrust being that both men 'should have known better' than to expect their affairs not to be exposed. In the case of *Ferdinand*, the judiciary appeared to imply that he should have curbed his behaviour and taken heed of the case of *Terry* and the disclosure of his teammate's infidelity.
[965] Auburn above, n 937 at 594.
[966] Akin to the case of *Rocknroll* above, n 960.
[967] See for example, *Peck* above, n 952.
[968] The 'personal public disclosure' scenario.

to take this into account. Perhaps what can be drawn from this is that the doctrine is fundamentally incompatible with the new erasure right.

Although the courts have failed to adopt Mills' approach to public domain discussed above, there has been some evidence to support the view that the English courts are taking a new approach to what constitutes the public domain, and a more liberal privacy-oriented one. As stated earlier, the traditional public domain 'test' has centred upon how many people know of the information in question.[969] However, in the recent case of *PJS*, the test for public domain shifted from that of knowledge – as it was found that the information in question *was not* in the public domain despite the fact that the information had been the subject of several articles outside of the jurisdiction and disseminated widely online.[970] The case concerned an interim injunction in respect of the publication of information about one half of a celebrity couple's extra-marital sex.[971] Despite the fact that rumours were rife about the claimant and his husband's sex life and the data in question had been published in the US, Scotland and Canada,[972] the UK Supreme Court reinstated the claimant's interim injunction.[973] A harm–based approach was taken in the case, the Court arguing that simply because there had been publications of a similar kind outside of the jurisdiction, this did not mean that more harm could not be done to the claimant and his family by further publications in the English and Welsh press.[974] An additional factor that seemed to justify the award of an injunction was that the private data in question had, in large part, been distributed online. Lord Neuberger expounded:

> '…a story in a newspaper has greater influence, credibility and reach, as well greater potential for intrusion, than the same story on the internet…'[975]

[969] For example, the focus of the court in *Terry* and *Ferdinand* was how many people both claimants had told about their affairs/how many people were aware.
[970] There is an abundance of US reportage on the rumours and the subsequent case. See for example a US article concerning the case on website 'Pop Goes the News' which had a disclaimer atop its website exclaiming that the blog is not bound by the injunction's English and Welsh jurisdiction: https://popgoesthenews.com/2016/05/19/uk-supreme-court-upholds-ban-on-naming-elton-john-and-david-furnish/ (last accessed 16/7/18).
[971] *PJS*.
[972] *PJS*.
[973] *PJS* [71] (Lord Neuberger).
[974] *PJS* [68] (Lord Neuberger).
[975] *PJS* [69] (Lord Neuberger) and see Butler above, n 982 at 454.

In essence, Lord Neuberger reasoned that stories printed in the traditional tabloid media are seen as more credible, reliable and truthful than information appearing online and therefore there was 'potential for intrusion' if the information were to be published in the English papers.[976] This sentiment can be disagreed with on its own terms. Given the prevalence of online news media, many people use the internet as a place where they can easily and quickly obtain information about current affairs (indeed all traditional printed press outfits now have large online presences). Even small websites that are outliers when compared with the traditional news media[977] have huge readerships and followings, attracting large amounts of people from a range of demographics.[978] Indeed, Lord Toulson disagreed with Lord Neuberger in this regard, arguing that it was important for the Lords not to be seen as 'out of touch of reality' and the 'world of public information is interactive and indivisible'.[979] Nevertheless, *PJS* may be said to have determined that even though information is widespread online, it can still retain a quality of privacy, in the sense that its further publication in the mainstream press can be viewed as capable of causing further harm. Therefore, the decision places a further limit on the use of the public domain doctrine.

There was undoubtedly a shift in focus of the Court in the case with regards to the doctrine – the Supreme Court's judgment focused upon the *type* of publication in question and *whether it would be believed.* Mead has also observed that the *nature* of the information concerned also now plays a role in whether the public domain doctrine is operable – the more private the information, the less likely it is that it will be found to be the public domain.[980] This is counter-intuitive, as the type of information is not necessarily related to whether it is already a matter of general knowledge. Perhaps what we are seeing here is a retreat of the court from the use of the public domain doctrine in MPI cases – Wragg has argued that a heavy reliance

[976] Oliver Michael Butler, 'Confidentiality and Intrusion: building storm defences rather than trying to hold back the tide' (2016) *The Cambridge Law Journal* 452, 454.
[977] And the traditional media's web presences: such as the news tab on *BBC.co.uk* and *The Guardian* online: both accessible at: https://www.bbc.co.uk/news and https://www.theguardian.com/uk (last accessed 16/7/18). An example of a popular outlier is *Buzzfeed* News: accessible at: https://www.buzzfeed.com/news?utm_term=.iyO3eqWWZ#.le2XYprrv (last accessed 16/7/18).
[978] The trial judge in *Monroe* did not accept that Twitter was the 'wild west' of social media and therefore people would not be persuaded by what was written on it – he noted that publication on social media can be just as damaging as those in the printed press (papers are often only read once anyway – so the internet is no more transient). See *Monroe v Hopkins* [2017] EWHC 433 (QB), [2017] W.L.R 68 [71(3)].
[979] *PJS* [89] and Butler above, n 976 at 454.
[980] The information in *PJS*, relating to sexual trysts, being inherently private in nature. Mead above, n 886 at 126.

on the factor makes such claims more akin to breach of confidence actions.[981] Butler comments upon the court's assessment of public domain in *PJS*:

> '…a shift from confidentiality or secrecy to *intrusion* permitted the court to move from a rather abstract notion of the "public domain" to a more concrete notion of the *harms* that disclosure in a particular location and medium would do to the claimant and his family.'[982]

This would appear to suggest a shift of the courts to a harm-based test. With regards to breach of confidence, Butler argues that the courts conduct an 'all or nothing' analysis: either the information is confidential, or it is not.[983] In contrast, the court in *PJS* conducted a claimant-centric approach including the consideration of where the data had been disclosed and the impact it had had on the claimant and his family.[984] Due to the uncertainty of the public domain doctrine as outlined above, a more nuanced approach to the doctrine is clearly needed in order to protect claimants. One could say that such an approach has been adopted in *PJS*. In establishing this, the amount of people that have viewed 'tweets' on Twitter has been seen as a contributing factor.[985] According to *Monroe*, over a thousand estimated views of a defamatory tweet, as well as other forms of engagement online was deemed to be 'substantial' enough as to cause reputational harm.[986] It is unclear whether a similar amount of people aware of the information in question would be viewed as enough to engage the public domain doctrine in MPI, particularly now that other factors such as the nature of the information and type of publication are considerations of the court.

Despite these qualifications, the implication of the doctrine still remains that if the information in question is to a significant extent public knowledge, an MPI claim may fail. The above section detailing contradictory judgments in MPI over the years serves to show that there is a large amount of definitional uncertainty surrounding what constitutes the *public domain* and how much influence the doctrine has. To conclude this discussion of the doctrine, it is important to restate several assertions that have been established. Firstly, and most generally, the public domain doctrine as broadly stated means that it is more difficult for a

[981] Wragg above, n 955 at 17.
[982] Butler above, n 976, 453 [emphasis added].
[983] Ibid 455.
[984] Ibid.
[985] *Monroe* above n 978 [54-62].
[986] Ibid.

claimant to mount a successful MPI action against information which is already widely present on *publicly accessible* websites online – regardless of whether or not a data subject has initially uploaded it themselves – although not impossible, as the judgment in *PJS* demonstrates. In a more universal sense, the doctrine itself is unclear: the old test for its operation appears to be 'whether there is anything private left to protect', however the Supreme Court in *PJS* appears now to be advocating a harm-based approach, taking into account considerations such as the intimacy of the data. Although this definitional uncertainty is problematic,[987] privacy advocates should welcome a more claimant-centric approach to the doctrine focusing upon reputational harm.

F. Remedies in MPI

I. Injunctions

Injunctions prohibiting the disclosure of personal information are an available remedy for MPI, along with compensation in the form of damages. On the face of it, injunctions in MPI can provide claimants with a significant amount of protection for their private data – and have served to do so in certain cases.[988] However, it will be argued here that for several reasons injunctions provide insufficient privacy-related protection *in practice*. The next section of this chapter will firstly explain different types of injunctions and the means of obtaining one, and then move to consider the difficulties that web-based dissemination has caused in terms of the efficiency of injunctions. The digital era has presented two central problems to the effectiveness of injunctions: firstly, the phenomenon of 'mass dissent' in flouting injunctions has flourished online with many people exposing those who have obtained injunctions on social media. It can be difficult to identify those who have initially broken an injunction or contributed to such dissent, as thousands of people can be involved and many use 'VPNs' to hide their true location and employ pseudonyms online. Secondly, injunctions only take effect within the jurisdiction of England and Wales. Many questions remain as to how to tackle the breach of an injunction on (for example) Twitter, which is based in the US and attracts multinational users from all over the globe.[989] As discussed

[987] It would of course aid a misuse claim with respect to intimate, online data. Article 17 does not specifically apply to intimate information.
[988] Perhaps the most notable recently being the claimant in *PJS*, their interim injunction upheld by the Supreme Court, as earlier discussed in this chapter.
[989] See the below discussion of *AMP v Persons Unknown* [20111] EWHC 3454 (TCC).

earlier in this chapter, salacious information already present online can also make it difficult to initially obtain an injunction. All of these issues were germane in *PJS*, which will be referred to in this section as a leading case.

Injunctions are an equitable remedy[990] and take the form of a court order prohibiting a particular action; in MPI cases, the order is normally a prohibition on the publication of certain facts. There are different types of injunctions available to claimants; a court may award an interim injunction before the MPI action has gone to trial. This order seeks to prevent the disclosure of certain private facts including, usually, the parties' names, pending the case being heard; the idea being that the 'status quo' is maintained before trial.[991] Interim injunctions are a crucial way of ensuring that a claimant maintains their Article 8 rights: once the information in question has been leaked to the public in a significant way, it would be unlikely that a court would uphold a long-term gagging order – its purpose already being defeated – in which case a claimant would only be able to obtain damages. As discussed below, damages, although providing a potential deterrent for publishers, do little to practically enforce personality rights.[992] 'Super-injunctions' can be awarded in the interim or long-term and are a more controversial form of injunction that not only prohibit publication of facts and/or party names but also bar the publication of any material that makes reference to the existence of the injunction itself.[993] Therefore, if a celebrity has successfully secured a super-injunction, the general public (in theory) would not know about it. 'Anonymised' injunctions are, as the name suggests, a prohibition on the reportage of party names to a case and are very commonly used in privacy cases, for obvious reasons. Publication of a story in a newspaper can compromise an injunction, breaching section 2 of the Contempt of Court Act 1981, the Attorney General having the power to bring proceedings. The Joint Committee on Privacy and Injunctions has urged the Attorney General to be vigilant in pursuing actions against breaches of injunctions online in the civil courts, the idea being that this would have a powerful deterrent effect.[994]

[990] Thaddeus Manu and Felipe Romeo Moreno, 'Is social media challenging the authority of the judiciary? Rethinking the effectiveness of anonymised and super injunctions in the age of the internet' (2016) 18(32) *Journal of Legal Studies* 39, 48
[991] Ibid, 48.
[992] This will be discussed in detail in the last part of this section.
[993] Although these types of injunctions are rare and if awarded primarily serve as an interim measure.
[994] Manu and Moreno above, n 990 at 58 and Privacy and Injunctions – Joint Committee on Privacy and Injunctions, chapter 4, paragraph 104, accessible at: https://publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/27307.htm (last accessed 12/10/18).

Section 12(3) of the Human Rights Act 1998 lays down the approach to be taken in deciding whether a court should award an interim injunction:

> 'No [relief which, if granted, might affect the exercise of the Convention right to freedom of expression] is to be granted so as to restrain publication before trial unless the court is satisfied that the applicant is *likely to establish* that publication should not be allowed.'[995]

The Civil Procedure Rules also give guidance on injunctions, the rules recommending that publicity is restricted when:

> 'publicity would defeat the object of the hearing; where the hearing involves matters relating to national security; where it involves *confidential information that may be harmed by publicity*; where it is necessary to protect the *interests of a child* or a protected party…'[996]

Section 12(3) replaced the previous test arising from *American Cynamid* that a claimant must have a genuine chance of success at trial; how this test appeared to work in practice was that if a claimant had an arguable case coupled with a 'balance of convenience' they could secure an interim injunction.[997] Phillipson has noted that there was an idea that under the *American Cynamid* test the courts were increasingly sympathetic to a claimant regarding interim publication restrictions, due to the fact that if a claimant's argument was not successfully made out at trial a newspaper outlet could ultimately publish their story afterwards, free from liability.[998] Section 12(3) of the Human Rights Act was therefore enacted because of the fear that Article 10 rights were being undervalued as a result of this approach – it set a higher threshold for such an award.[999] The current test is set out in the case of *Cream Holdings*:

> 'the general approach should be that courts will be exceedingly slow to make interim restraint orders where the applicant has not satisfied the court he will probably ("more

[995] Human Rights Act 1998 [emphasis added].
[996] Manu and Moreno above, n 990 at 52 and see 'Procedure Rules, Part 39: Miscellaneous Rules Related to Hearings' available at: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part39#39.2 (last accessed 12/1/0/18), part 39.2 [emphasis added].
[997] Gavin Phillipson, 'Max Mosley goes to Strasbourg: Article 8, claimant notification and interim injunctions' (2009) 1(1) *Journal of Media Law* 73 and *American Cyanamid Co v Ethicon Ltd* [1975] AC 396.
[998] Ibid.
[999] Ibid.

> likely than not") succeed at the trial. In general, that should be the threshold an applicant must cross…But there will be cases where it is necessary for a court to depart from this general approach and a lesser degree of likelihood will suffice as a prerequisite'.[1000]

Cream Holdings then provides that if a claimant appears *on the balance of probabilities* likely to win their case, then an interim injunction will be awarded.[1001] Courts perhaps remain wary of awarding an interim injunction to a claimant who ultimately may not be able to establish their case at trial.[1002] Clearly, the court must make a judgment as to the award of an injunction which creates a fair balance between privacy and free expression. If the test were to be made stricter so that an interim injunction would not be awarded where there was a chance that it would not be maintained at final trial, it is argued that that balance would not be maintained since the privacy of the information would be lost before full argument could be heard as to the strength of both claims, rendering it virtually pointless for the claimant to pursue the case any further.

i. Section 12(4) of the Human Rights Act and IPSO

Section 12(4) of the Human Rights Act also contains material of relevance to remedies in MPI. It states:

> '(4) The court must have particular regard to the importance of the Convention right to freedom of expression and, where the proceedings relate to material which the respondent claims, or which appears to the court, to be journalistic, literary or artistic material (or to conduct connected with such material), to—
>
> (a)the extent to which—
>
> (i)the material has, or is about to, become available to the public; or
>
> (ii)it is, or would be, in the public interest for the material to be published;

[1000] *Cream Holdings Ltd v Banerjee and Others* [2005] 1 AC 253 [22].
[1001] See also *NPV v QEL and ZED* [2018] EWHC 703 (QB). Manu and Moreno have argued that the new standard means that claimants must show that 'irreparable' harm would be caused to them if such an injunction were not granted but this is plainly a minority view: Manu and Moreno, above n 990 at 50.
[1002] Ibid, 53.

(b)any relevant privacy code.'[1003]

As above in relation to section 12(3), the Supreme Court has stated that section 12(4) does not mean that Article 10 will take precedence over Article 8.[1004] Again, prior to the case of *PJS* this had been an issue of contention, with Jack Straw MP stating to parliament that he hoped the inclusion of section 12(4) in the Act would mean that injunctions were only granted in exceptional circumstances.[1005] Section 12(4)(b) stipulates that when considering injunctive relief, the court must also take into account any relevant privacy code.[1006] The respondents in *PJS* were subscribed to the Independent Press Standards Organisation (hereafter 'IPSO'). IPSO was formed after the Press Complaints Commission finished operations in 2014 and IPSO adopted the Commission's Privacy Code for Editors. The Code states that everyone has the right to 'respect' for their private and family life and lists various factors to be taken into account when weighing privacy interests against expression rights.[1007] The Code notes in relation to the public interest:

'2. There is a public interest in freedom of expression itself.[1008]

3. Whenever the public interest is invoked, the PCC will require editors to demonstrate fully that they reasonably believed that publication, or journalistic activity undertaken with a view to publication, would be in the public interest.

4. The PCC will consider the extent to which material is already in the public domain, or will become so.'[1009]

It is interesting to note that the 'public domain' factor is present in the Code; however, this still did not preclude the Court's award of an injunction to the claimants in *PJS* – despite the fact that the information in question was (to an extent) public knowledge. This raises the

[1003] Human Rights Act 1998.
[1004] *PJS* [33].
[1005] Manu and Moreno, above n 990 at 52. Presumably, this means that Straw believes that injunctions should be awarded only when intrusion on the private life of a claimant would have extraordinarily serious ramifications.
[1006] Human Rights Act 1998.
[1007] See Editors' Code of Practice, Independent Press Standards Organisation, available at: https://www.ipso.co.uk/editors-code-of-practice/#Privacy (last accessed 15/10/18).
[1008] Fortunately, the controversial inclusion of this factor into the code has largely been ignored by the judiciary. See Gavin Phillipson, 'Leveson, the Public Interest and Press Freedom' (2013) 5(2) *Journal of Media Law* 220.
[1009] See Editors' Code of Practice, IPSO above, n 1007.

question of how influential or powerful the Code is in judicial decision-making.[1010] That being said, two factors may have encouraged the Court's decision to provide an injunctive award in that particular case. First is section 5 of the Privacy Code which states:

> '5. In cases involving children under 16, editors must demonstrate an exceptional public interest to over-ride the normally paramount interest of the child.'[1011]

This part of the Code is referring to cases where the claimant is a child, such as in *Murray* and *Weller*.[1012] The couple in question in *PJS* had two young children, a higher threshold therefore being required for respondents in proving a genuine public interest value in the material (which they ultimately did not satisfy).[1013] Secondly, the Press Complaints Commission's guidance in 2011 on 'Privacy and Social Networking' stated:

> 'newspapers cannot automatically justify the use of material simply on the basis that it has appeared previously on the internet and is, therefore, 'publicly available'. Even if an individual has not taken steps to protect their personal information (by hiding it behind strict privacy settings), newspapers will have to consider whether republication of the material shows respect for the individual's privacy.'[1014]

According to this logic, an online outlet having reported on the sex-life of a claimant would not necessarily bar the award of an interim injunction (which was the outcome of the Supreme Court's decision). *PJS* shows that the Code has a limited impact on the outcome of MPI cases and many of the clauses within the Code relating to private life have public interest exceptions. This raises the question of how powerful the Code is in protecting privacy interests – how effective the guidance is in this regard depends upon how broadly a judge interprets these exceptions. While on the face of it the Code serves to protect Article 8 rights, it may not be as robust a safeguard as claimants may wish. This also applies to privacy codes other than that officially adopted by IPSO. In *Sir Cliff Richard*, Mr Justice Mann took

[1010] The code was referred to extremely briefly in *PJS*: see [36].
[1011] See Editors' Code of Practice, IPSO, above, n 1007.
[1012] *David Murray* above, n 838 and *Weller* above, n 842.
[1013] *PJS* [36].
[1014] See 'PCC Ruling: Twitter, Journalism and Privacy' (1st March 2011) available at: http://healthyhomenepal.com/1598-article.html (last accessed 15/10/18).

into account the BBC's own privacy code or 'Guidelines', despite the fact he did not feel they advanced any debate.[1015]

The decisions of both the Court of Appeal and the Supreme Court in *PJS* serve as contemporary examples of how the English courts approach the award of a privacy injunction. As discussed earlier in this chapter, the claimant had applied for an interim injunction in respect of information that a news outlet wished to disclose regarding his extra-marital sexual liaisons.[1016] The Supreme Court upheld award of an interim injunction in respect of this information for several reasons. Firstly, the Court held that newspaper hard-copy coverage of the claimant's sex-life would negatively affect the claimant and his young family to the point where it made the trial itself redundant.[1017] The court also observed that although there had been some coverage of the facts in question online this was not decisive – this once again signifies a more liberal or relaxed approach to the public domain doctrine, a shift discussed earlier in this chapter.[1018] Using *Cream Holdings*, the court argued that the publication of information would invade the privacy rights of the claimant as it concerned his sex-life and there was no significant public interest argument advanced by the respondents.[1019]

ii. *PJS* and section 12(3) of the Human Rights Act

The Court of Appeal in *PJS* also made some interesting observations regarding section 12(3) of the Human Rights Act. It noted that it 'raised the bar' as to what it was required for a claimant to prove in order to secure an interim injunction – something that was not disputed by academics or the Supreme Court.[1020] However, the Court of Appeal also found that section 12(3) meant that Article 10 interests must be *prioritised* over those of Article 8 with regards to interim injunctions – that Article 10's weight was 'enhanced'.[1021] This aspect of the interpretation of section 12(3) was eventually disapproved of by the Supreme Court, the Court noting that this in itself was a reason that the Court of Appeal's decision should be re-

[1015] *Sir Cliff Richard* [306].
[1016] *PJS*.
[1017] *PJS* [1].
[1018] See above.
[1019] *PJS* [2] (Lord Mance).
[1020] Phillipson above, n 997 and *PJS* [19].
[1021] *PJS* [40].

evaluated.[1022] The Supreme Court held that the balancing exercise must treat both rights as having *equal weight* and if both are in conflict an intense focus on the particular facts would be necessary along with a view as to proportionality.[1023] This robust statement of the Supreme Court could be said to put to bed any debate about the relative importance of Articles 8 and 10 – England and Wales' most senior court has definitively stated that neither right has precedence over the other in respect of the award of injunctions.

iii. Other factors relating to the award of an injunction

Caselaw prior to *PJS* has provided other relevant factors that could be considered by the courts when deciding whether to grant an injunction. Lord Justice Sedley in *Douglas v Hello* refused the claimants an interim injunction, stating that he was not convinced that their right to privacy in the case would tip the balance against expression; the claimants were a celebrity couple wishing to restrict the publication of photographs of their wedding, having signed an exclusive contract with a different publication other than the defendants.[1024] This suggests that a motive of financial gain will not hold a great amount of weight to section 12(3) of the Human Rights Act being satisfied. *A v B Plc* in 2002 found that if a publication can be legitimately put on hold with little detrimental impact to its public interest value this could *support* an application for an interim injunction.[1025] An example of such a scenario would be information about Max Mosley's sexual proclivities: there is no time restraint on how public interest-worthy information such as this would be. A delay of a few months in publishing information like this would have had no impact on its newsworthiness.[1026] The 'children factor', although discussed above, must again be emphasised here due to its importance: if a claimant has a young family then this often helps their application for an interim injunction or a long-term anonymous injunction. This has been the case in many instances such as *Weller*, *PJS* and *ETK v NGN*.[1027] The idea behind this appears to be that if children could be negatively affected by the release of certain personal information about their parents (for example by bullying at school) then this should be stopped. This principle can be likened to that in the tort of *Wilkinson v Downton* that protects against emotional as well as physical

[1022] *PJS* [20].
[1023] *PJS* [20].
[1024] *Douglas v Hello* [2001] Q.B. 967 (CA).
[1025] [2002] EMLR 7 (QB).
[1026] Phillipson above, n 997.
[1027] See for example *ETK v News Group Newspapers Ltd* [2011] EWCA Civ 439 and *PJS*.

harassment.[1028] In the case of *Rhodes v OPO,* the publication of a memoir was objected to on the grounds that the son of the person concerned would suffer mentally as a result.[1029] The presence of blackmail in a case can also act to support the award of an injunction.[1030] However, the bare fact of a relationship, Agate has argued, may not attract sufficient privacy-related protection to justify the award of an injunction, although any salacious details would be likely to be prohibited from publication unless found to be in the public interest.[1031] Indeed, Lord Mance in *PJS* highlighted that 'kiss and tell stories' have no public interest value.[1032]

This section of this chapter has attempted to outline different types of privacy injunctions as well as some of the process that a claimant must go through in order to obtain one – a lengthy and arduous one. Although injunctions do play a role in suppressing the publication of personal and private information, they have two fundamental shortcomings in effectiveness that have been exacerbated by the digital age. These shortcomings will be discussed next.

II. The shortcomings of injunctions in misuse of private information and information online

i. mass dissent against privacy injunctions

The first key shortcoming of injunctions as a remedy in MPI is the prevalence of public 'mass dissent' from court awards of injunctions and anonymous online disclosure as to the recipients. The nature of the internet lends itself to people breaking injunctions *en masse*, dissemination online being largely free, quick and easy. Many people now have some kind of social media account and a pack mentality can reign online, especially when a topic is 'trending' or speculation is rife over a certain issue. It is also common practice to re-share information on social media websites (Twitter installing a one-click 're-Tweet' button) so it

[1028] [1897] EWHC 1, [1897] 2 QB 57.
[1029] [2015] UKSC 32. It should be noted that in the Supreme Court, the injunction that prohibited the publication of the memoir was overturned.
[1030] *NPV* above, n 1001.
[1031] Jennifer Agate, 'Does the internet make it too easy to pick up the pieces? Goodwin, jigsaw identification and intrusion into sexual relationships' (2011) *Entertainment Law Review* 246, 247 and *Goodwin v NGN Ltd* [2011] EWHC 1437 (QB) [2011] EMLR 27 (QBD).
[1032] Keina Yoshida, 'Privacy injunctions in the internet age – PJS' (2016) 4 *European Human Rights Law Review* 434, 435.

travels further. Indeed, a video of Max Mosley being spanked by prostitutes had been viewed 1.5 million times before his application for an interim injunction.[1033] His application for an injunction was unsuccessful on this basis – there was nothing private left to protect, and even its removal from the News of the World's website would not stop its spread[1034] as it had likely already been shared to a vast number of other websites.[1035]

Super-injunctions have been a particular target for this widespread dissent in the sense that groups of people have gathered to expose celebrities holding such injunctions on social media. The press have indirectly encouraged this mass dissent: Agate notes that in past cases, the press have consented to an injunction with a claimant (or simply have not opposed an injunction) yet contemporaneously ran inflammatory headlines complaining about lawyers' 'scuppering' free speech and dropping heavy hints as to who the beneficiary of the injunction might be.[1036] This came to a head in 2011 to the extent that it was branded 'the 2011 British privacy injunctions controversy' and website Wikipedia has a page dedicated to it.[1037] This phenomenon of dissent and defiance of court orders appeared to be successful because of the idea of 'strength in numbers' (ie. if hundreds or thousands of people have breached a gagging order, there is no more to fear if an individual does it himself or herself). The mass public outcry seemed to stem from the idea that injunctions were unjustly interfering with free speech or freedom of the press. This public dissatisfaction peaked when John Hemming MP used parliamentary privilege (protecting himself from legal sanctions) to 'name and shame' two public figures who had obtained privacy injunctions, including footballer Ryan Giggs, whose name and association with the legal case was also being readily disclosed on Twitter. News sites online soon followed after Hemming had burst the dam and the information was repeated more than 75,000 times.[1038] In light of the scandal (and perhaps wary of his own injunction being exposed) TV presenter Jeremy Clarkson lifted his own injunction in October

[1033] Phillipson above, n 997.
[1034] Ibid.
[1035] It should be noted that the right to be forgotten, as an *ex post* right, may also face this problem – a claimant may have found that their private information has travelled to multiple sites by the time they are looking to have the information erased. However, a deletion request, even if made to several websites or a search engine, would likely take less time than mounting an expensive and lengthy proceeding in MPI. See the discussion of the case of *AMP* below.
[1036] Jennifer Agate, 'Battle lines drawn: privacy injunctions following CTB et al' (2011) *Entertainment Law Review* 212, 213.
[1037] Accessible at: https://en.wikipedia.org/wiki/2011_British_privacy_injunctions_controversy#Jeremy_Clarkson) (last accessed 15/10/18).
[1038] Manu and Moreno above, n 990 at 62.

of 2011 that prohibited exposure of an extra-marital affair. Clarkson stated that he believed that privacy injunctions were worthless in an interview with *The Daily Mail*:

> 'You take out an injunction against somebody or some organisation and immediately news of that injunction and the people involved and the story behind the injunction is in a legal-free world on Twitter and the internet. It's pointless.'[1039]

As recently as last year, Lord Peter Hain named Arcadia mogul Sir Philip Green as the man who had obtained an injunction against *The Daily Telegraph* to prevent the disclosure that former employees had accused Green of sexual and racial harassment.[1040]

Although such breaches are illegal, the sheer amount of those doing it makes it difficult to stop the wave of disclosure. Senior lawyer Jennifer Agate summarises the practical problems with mass dissent against injunctions online:

> 'Contempt of court occurs when a publication, written or spoken, tends to interfere with the course of justice in particular legal proceedings, regardless of intent to do so. Thus every one of the estimated 30,000 twitter users who identified CTB is liable to prosecution, whether they understood the laws they were breaking or not. Would it be in the public interest to prosecute every one of them? *Obviously not*.'[1041]

Agate has argued that because it is difficult if not impossible to sue everyone individually who has engaged in mass dissent it is more efficient to go to the source of the dissent – the social media websites themselves, or host websites.[1042] This is a similar action that individuals take when seeking to prevent on copyright infringement – the copyright holder will take action against a host streaming site.[1043] Accordingly, Twitter – the social media website often at the centre of this mass dissent – released a response to the (illegal) revelation

[1039] See for example Josh Halliday and Agencies, 'Jeremy Clarkson lifts 'pointless' injunction against ex-wife' (*The Guardian* , 27 October 2011) accessible at: https://www.theguardian.com/media/2011/oct/27/jeremy-clarkson-lifts-injunction?newsfeed=true (last accessed 15/10/18).
[1040] See 'Sir Philip Green hits back at Lord Hain for injunction breach' (*BBC News*, 27 October 2018) accessible at: https://www.bbc.co.uk/news/uk-45999197 (last accessed13/8/19) and see Paul Wragg, 'Lord Hain and Privilege: When power, wealth and abuse combine to subvert the rule of law' (*Inforrm*, 27 October 2019).
[1041] Agate above, n 1036 at 214. Emphasis added.
[1042] To some extent this problem has been addressed by AMP in the form of group injunctions - see the discussion of AMP below.
[1043] Agate above, n 1036 at 214 [emphasis added]. Section 5 Defamation Act 2013 also takes this approach as to third party posting of defamatory content online.

on its platform that Ryan Giggs held a super-injunction. Its head of public policy in 2011 released a statement explaining that the platform was intending to restrict tweets as only accessible in certain countries if they had been flagged by a reputable authority as breaching an injunction.[1044] Although this attempt at dealing with the problem of dissent should be welcomed, there are several flaws in Twitter's proposed solution. Firstly, the effectiveness of reporting could be a potential issue: will there be designated 'reporters' lurking on social media in lieu of a super-injunction, and how many will there be? Questions may also be raised as to what is classed as a reputable body. There is likely to be a gap in time between when a tweet is reported and access to it restricted, by which time it will have been seen by a number of people (possibly thousands or even millions, depending upon how long the time gap was and how high-profile the 'Tweet-er' is).[1045] It is unclear what is to be done if the tweet in question has been spread more widely around Twitter – if it has been 're-tweeted' or the information written in an entirely new tweet, rather than a link copied. There is also the issue of someone using a VPN to shift their location from England to elsewhere – this would mean that they could have access to the tweet in question through another country's Twitter feed. Finally, and most obviously, the issue of dissent towards super-injunctions spans the web and is not exclusive to Twitter as a platform. Other platforms, including news websites, often employ a word-based filter in order to stop certain comments appearing on their websites.[1046] There are further problems with this type of remedy – a word filter would often block only certain pre-ordained universally offensive words. It is unlikely that such a filter could be programmed to block the mention of the actual names of every claimant who has taken out an injunction, and even if this was done, it could actually alert suspicion in social-media users as to who in fact has obtained one.[1047]

ii. AMP v Persons Unknown

The case of *AMP v Persons Unknown* in 2011[1048] sheds some light on how the problems of anonymous disclosure over multiple webpages can begin to be tackled by the judiciary in an

[1044] See 'Twitter could block super-injunction tweets' (*The Daily Telegraph,* 30 January 2012), accessible at: https://www.telegraph.co.uk/technology/twitter/9050047/Twitter-could-block-super-injunction-tweets.html (last accessed 17/10/18). Professor Helen Fenwick highlights this in her course 'Media Law' at Durham Law School, Durham University.
[1045] This is also a problem embodied by the right to erasure.
[1046] See *Delfi AS v Estonia*, App no 64569/09, (ECHR, 16 June 2015) hereafter '*Delfi 2015*'.
[1047] If, for instance, they had attempted to tweet about the person in an unrelated capacity and found their post was blocked or restricted.
[1048] *AMP v Persons Unknown* [2011] EWHC 3454 (TCC).

MPI claim. The case concerned a woman who had had her phone stolen while away studying in 2008. Crucially, the phone did not have a password to stop material on the phone being accessed when out of her hands and the phone's memory contained explicit photographs of the claimant that she had taken for her boyfriend.[1049] Not long after the theft of her mobile phone, these explicit photographs appeared on a 'free media hosting service' and the claimant was successful in removing these pictures by contacting the service. Her friends and family alerted her to the pictures' presence as her Facebook account details had been attached to the pictures.[1050] In November of 2008 the matter came to a head and the pictures were uploaded again to a Swedish website that hosts 'BitTorrent' files[1051] and her name was connected to each image so, when the claimant's name was searched online, these images were near the top of the search results.[1052] The claimant successfully removed some of the links to these images (in the US) using the US' Digital Millennium Copyright Act, and the action in *AMP* related to the claimant seeking to obtain control over this information inside the English and Welsh courts' jurisdiction.[1053]

Andrew Murray of the London School of Economics gave expert evidence and advised the Court as to the appropriate remedy in order to stop information flow. He explained that due to the nature of BitTorrent, it would be possible to trace 'seeders' (people who have downloaded pieces of the file, and due to its programming, allow pieces of the file through their download to once again be re-uploaded and the data promulgated) using their IP addresses obtained from internet service providers.[1054] Murray also stated that: 'given the characteristics of the claimant' it was 'unlikely that many of the seeders will be outside the jurisdiction of this Court.'[1055] In other words, Murray was making an educated guess that a lot of seeders were based in England and Wales and he noted that due to the design of BitTorrent, even if some of them were not, enough would have been 'taken out' to stop the spread of the data (there would not be enough fragments being uploaded to make a file). A notable aspect of the decision is that the judge, in order to stop the claimant having to re-file her case, granted a general injunction to 'persons unknown' – in other words, to a class of

[1049] Ibid [4-5].
[1050] Ibid [6].
[1051] Ibid [8].
[1052] Ibid.
[1053] Ibid.
[1054] Ibid [9-15].
[1055] Ibid [16].

people who possessed any part of the file[1056] – therefore avoiding the problem of anonymous posting.[1057] In granting the injunction, the judge relied upon Article 8 ECHR and MPI case law, including *Campbell*, and found that the claimant had a reasonable expectation of privacy in respect of the photographs.[1058]

This case serves to show that through the ingenuity of an enterprising judge, MPI can in fact be utilised in order to combat the distribution of private data online, even if those posting the data are anonymous (and numerous). However, it is important that the significance of this case is not over-stated. The decision is in some ways unique to its facts as it concerns BitTorrent – where information is uploaded through the combination of multiple seeders combining forces and downloading pieces of the information (and spreading it further) rather than a situation whereby the picture itself has been uploaded *in its entirety* to different sites by multiple individuals online. Therefore, if a proportion of the seeders are inside the jurisdiction (England and Wales) then this ruling will stop their part in the process – so the data cannot be accessed *as a whole*. This ruling would not have had the same effect if the pictures in question were uploaded to, say, a German website as a whole by individuals outside of the court's jurisdiction.[1059] Additionally, the case facts themselves are more akin to an action in revenge pornography than a standard MPI claim, and there is some evidence in the Court's judgment that the claim was taken more seriously for this reason – perhaps why the Court was so keen to 'strike a blow' in favour of privacy rights.[1060] Whether such an order would have been granted in a more standard privacy action (or one that did not involve explicit pictures and malice) is unclear. Further to this point, the judgment referenced the Protection of Harassment Act 1997 in addition to MPI case precedent. This would not always be applicable in MPI cases with respect to private data online. Indeed, Murray noted that the claimant's legal team:

[1056] The seeders in the bittorrent scheme.
[1057] Ibid [19-21].
[1058] Ibid [24-28].
[1059] In contrast, in this circumstance, the right to be forgotten under the GDPR could now be used. Andrew Murray has however noted that he had been informed that that across Europe, there is a potential for a European arrest warrant to be used in order to enforce this order beyond England and Wales, although he does not flesh this possibility out – see: See Andrew Murray, 'New Approach to Privacy: AMP vs Persons Unknown' (*The IT Lawyer*, 20 December 2011), accessible at: http://theitlawyer.blogspot.com/2011/12/new-approach-to-privacy-amp-v-persons.html (last accessed 12/8/19).
[1060] As Louise Mensch MP stated on the ruling. See Andrew Orlowski, 'Judge bans stolen student sex pics sharing on BitTorrent' (*The Register*, 12 January 2012) accessible at: https://www.theregister.co.uk/2012/01/12/amp_bittorrent_injunction/ (last accessed 14/8/19).

> '…developed a number of claims including claims under the Copyright, Designs and Patents Act 1988 but essentially it came down to two claims: (1) Privacy under Article 8 of the ECHR and (2) Protection from Harassment. **The stronger claim was under the Protection from Harassment Act 1997** as an infringement of a harassment order is a criminal offence'.[1061]

Murray has written that he believes this trial did not involve a 'free speech issue' – this is not the case, however, with regards to other types of privacy claim.[1062]

iii. Decisions to award injunctions in the digital age

Various arguments have been run in MPI cases as to whether an injunction should be awarded by the courts if there has been disclosure of the information in question online either *before* the award of an injunction or afterwards, in a 'dissenting' move. The Supreme Court in *PJS* stated its position:

> 'In the circumstances, Eady J held that even identification should not be permitted. It will be apparent that the circumstances in CTB bore some relevant similarities to those of the present case. In particular, reliance was placed on internet disclosures subsequent to the original injunction in support of an application to set aside the injunction on the basis that it served no further useful protective purpose. This situation was distinguished in principle from that where an injunction is granted after substantial internet disclosure. The substantial internet disclosure which had occurred *after the injunction was not regarded as justifying the lifting of the injunction.* The injunction, enforceable against the defendant, was seen as continuing to serve a useful purpose.'[1063]

In essence, the Supreme Court waded into this debate and stated that courts are more likely to uphold an injunction when dissenters online are attempting to sabotage its award by disseminating private information in an intentional way. The Court here also implied that it

[1061] See Murray above, n 1059 [emphasis added].
[1062] Ibid. And indeed other types of deletion request that could be brought under the right to be forgotten.
[1063] *PJS* [20]. Emphasis added.

may be more reluctant to award an injunction if the information was available online prior to a hearing; however the outcome of *PJS* was to decide to uphold an injunction granted in just such a circumstance.[1064] The thrust of the judgment appears to be that those wishing to deliberately flout an injunction online will not be able to hold the court to ransom. The Supreme Court also made some interesting comments regarding the purpose of an injunction in the digital era. The Court once again highlighted the key notion of intrusion and asked the question of whether the information, as disclosed more widely, would intrude further on an applicant's private life, in a claimant-centric approach:

> 'Mr Tomlinson argues accordingly that "the dam has not burst". For so long as the court is in a position to prevent some of that intrusion and distress, depending upon the individual circumstances, it may be appropriate to maintain that degree of protection'.[1065]

As discussed earlier in this chapter, the Court went on to note that the publication of the information in national newspapers was more intrusive and damaging than publication online.[1066] This approach was also echoed in the case of *Goodwin*:

> 'However, the degree of intrusion caused by internet publications was, Tugendhat J. felt, different from the degree of intrusion caused by print and broadcast media. Important though the story was, he said, there were many people who would not take the trouble to find out from VBN's job description what her name was.'[1067]

Courts may feel that they must take this position through sympathy to a claimant as they are unable to award injunctions which are futile.[1068] Paying homage to this principle does not, in actuality, make injunctions any more effective in stopping the spread of personal information online. The point to be taken from this sub-section is that courts are striving to continue to award injunctions in an attempt to protect claimants despite their lack of effectiveness in the digital age. This is perhaps through lack of a better alternative – as this thesis has argued, one may be present in the right to erasure.

[1064] *PJS* [67-71], [72], [78] and [92].
[1065] *PJS* [29].
[1066] *PJS* [29].
[1067] Agate above, n 1031 at 248.
[1068] See *PJS* [30].

iv. Ineffectiveness due to territorial scope

The second reason that injunctive relief is ineffective in the online sphere is because of the limited territorial scope of privacy injunctions. Individuals who are active online often host their websites on US servers in an attempt to escape the jurisdiction of England and Wales and to make it more difficult for injunctions to be levelled against them.[1069] If they are based outside of the jurisdiction, it becomes more expensive to take action against them and, at least in the US, the First Amendment will prevent any privacy injunction being enforced.[1070] Injunctions awarded by courts in England are also weakened by the split jurisdiction within the UK – as Manu and Moreno have observed, 'Section 18(5)(d) of the Civil Jurisdiction and Judgments Act 1982 provides that an interim measure (including an injunction) obtained in one of the UK's jurisdictions is not enforceable in the other jurisdictions.'[1071] As was seen in the case of *PJS*, Scottish publications flouted the initial injunction put in place by an English court.[1072] The courts have repeatedly argued that if an injunction is pointless or in vain (be it due to jurisdictional issues or otherwise) they will refuse to award one, even if they have sympathy with a claimant. The potential for an injunction to be in vain has increased because of the disclosure possibilities on the internet. Lord Justice Eady noted in the 2008 case of *Mosley*:

> '…if someone wishes to search on the Internet for the content of the edited footage, there are various ways to access it notwithstanding any order the Court may choose to make imposing limits on the content of the *News of the World* website. The Court should guard against slipping into playing the role of King Canute. Even though an order may be desirable for the protection of privacy... It is inappropriate for the Court to make vain gestures.'[1073]

[1069] Manu and Moreno above, n 990 at 62.
[1070] Ibid at 62.
[1071] Ibid.
[1072] Ibid 63-64 and *PJS.*
[1073] *Mosley v NGN* above, n 953 [33-34].

The Court of Appeal emphasised this point in its judgment in *PJS*, stating that it would not make an order that it deemed 'ineffective'.[1074] Jurisdictional issues undoubtedly make injunctions less effective: devices can be employed in order to search for content hosted on servers outside of the English and Welsh jurisdiction, for example by using 'Spanish Google'.[1075] Data is often disseminated indiscriminately across the web both inside and outside of a jurisdiction and the dark web (a large section of the internet) remains unregulated. Indeed, some academics have argued that the injunction upheld by the Supreme Court in *PJS* was futile for this reason.[1076] The Court of Appeal differentiated the problem of media defiance towards injunctions and commented in a somewhat defeatist fashion that 'the Internet and social networking have a life of their own'.[1077] The problem of anonymity in posting compounds the issue of data travelling across borders, as this makes the identity of an 'end-user' elusive.[1078]

This section has made several points with regards to injunctions under MPI. Firstly, the judiciary are attempting to uphold the award of injunctions on the grounds of 'intrusion' in the digital age, despite the problems that a technological world presents. Two of these problems are the phenomenon of mass dissent in breaking injunctions on social media and other web platforms and the cross-border nature of the internet, making it possible to post and access injuncted information outside of one's jurisdiction.[1079]

II. Damages as a remedy in misuse of private information

The other remedy available in MPI is damages, or monetary compensation. Max Mosley, after being awarded £60,000 in the English courts, took a case to Strasbourg arguing (amongst other matters) that damages were not an adequate remedy for infringing privacy rights. The ECtHR stated:

> 'in its examination to date of the measures in place at domestic level to protect article 8 rights in the context of freedom of expression, it has implicitly accepted that ex post

[1074] *PJS* [47].
[1075] See *Google Spain.*
[1076] Manu and Moreno above, n 990 at 43.
[1077] *PJS* [45].
[1078] Manu and Moreno above, n 990 at 61.
[1079] Although this is by no means an exhaustive list – there are doubtlessly other problems which it goes beyond the scope of this thesis to discuss.

> facto damages *provide an adequate remedy* for violations of article 8 rights arising from the publication by a newspaper of private information.'[1080]

Despite this finding, arguments have persisted that damages are an insufficient remedy for this type of claim. Damages are an award for *injury to feelings*[1081] without actually being able to remedy this injury in a meaningful way. One can argue that the possibility of damages being awarded against a defendant serves as a deterrent effect to publishers. However, on examination of the relatively small amount of damages that have been awarded in MPI cases, this theory appears weak. In *Campbell*, the claimant was awarded £2,500, in *Douglas* the award was £14,600 and in *McKennitt* £5,000.[1082] Despite Mosley's award being more significant than those in previous cases, Mr Justice Eady in the case recognised that the sum would still not constitute redress:

> "... I have already emphasised that injury to reputation is not a directly relevant factor, but it is also to be remembered that libel damages can achieve one objective that is impossible in privacy cases. Whereas reputation can be vindicated by an award of damages, in the sense that the claimant can be restored to the esteem in which he was previously held, that is not possible where embarrassing personal information has been released for general publication…'[1083]

In 2018 Mr Justice Mann awarded Sir Cliff Richard £210,000 in damages for winning his MPI suit against the BBC (in conjunction with South Yorkshire Police). This represents a significantly larger sum than was awarded the aforementioned cases, which was in part due to the presence of aggravated damages[1084] but also because the judge's assessment of the general damages had been (comparatively) generous. Mr Justice Mann justified the award of this figure due to a combination of powerful factors, including the significant amount of intrusion and distress that Sir Cliff had endured due to the publication, the highly damaging nature of the private content revealed, the broad scope of the publication and the sensationalist presentation of the publication.[1085] Arguably, Sir Cliff was in an extremely

[1080] *Mosley v UK* App No. 48009/08 (ECHR, 10 May 2011) [emphasis added].
[1081] See *Campbell.*
[1082] *Campbell*, *Douglas* (*No.2)* above, n 923 and *McKennit v Ash* above, n 831.
[1083] *Max Mosley v NGN* above, n 953 [230-231].
[1084] *Sir Cliff Richard* [365]. The factor which 'aggravated' the claim was that the BBC had entered the Sir Cliff Richard story into a competition for it to win 'scoop of the year'.
[1085] *Sir Cliff Richard* [350-7].

strong position regarding his MPI claim due to the facts of his case; in theory then, this figure represents the upper echelons of what a claimant could expect to receive when winning an action. Special damages were also awarded in the case.[1086]

As stated above, in defamation, a claimant can regain at least some of their former standing if they win a case as it is publicly proclaimed that they have been defamed using false facts. In contrast, as Mr Justice Eady has observed, once information has been published in MPI it is almost too late – the dam has burst and money will do little to rectify this. There is the additional problem of the 'Streisand effect'; many claimants decide not to pursue an action in MPI if the data has (to some extent) already been made public as paltry damages are not worth prolonging the pain and negative publicity drawn to the data leak. Litigious claimants like Max Mosley in this field are rare.[1087] In Mosley's case, Mr Justice Eady did not make an award of punitive damages – this would have set controversial precedent – but ordered that the substantial legal fees of Mr Mosley would be paid by the respondents, amounting to £850,000. Therefore, an award of costs against a publisher can often have more of a deterrent effect than the award of damages. It is possible for a claimant to be awarded aggravated damages in MPI to compensate for 'special dignity harm' and Hunt has observed that the Strasbourg Court has *not* stated that this interferes with Article 10 rights.[1088]

A final point of interest arising from Mosley's 2011 ECtHR case was that the Court held that pre-notification for claimants as a requirement imposed on publishers (prior to publication) would be difficult to work in practice and may breach Article 10.[1089] Phillipson has argued that there are three problems with the lack of a pre-notification requirement:

- In modern times, editors are now less likely to pre-notify (based on anecdotal evidence);

- There is an incentive for an editor *not to do so* – they want the story to run and sell papers, and they are not obliged to;

[1086] *Sir Cliff Richard* [370-428].
[1087] Chris Hunt, 'Strasbourg on Privacy Injunctions' 70(3) (2011) *Cambridge Law Journal* 489, 490.
[1088] Ibid, 491.
[1089] *Mosley v UK* above, n 1080 [117].

- An editor knows that if they publish the story in a paper's edition before a claimant is aware, they are less likely to take an action in MPI after the fact because the information is already out there – and damages would be likely to be modest if awarded at all.[1090]

Due to these reasons, the lack of a pre-notification requirement compounds the problem of insignificant monetary damages afforded to claimants in MPI cases. A pre-notification requirement may allow a claimant to secure a long-term injunction that could result in their Article 8 rights being protected (pending dissent online). If information is printed before a claimant can take court action then the only remedy that a claimant may receive is damages – and a small amount of them. This does exceedingly little to uphold personality rights in the digital age.

i. Comparing MPI, injunctions and the right to be forgotten

The purpose of this chapter has been to demonstrate the shortcomings of MPI and its remedies in relation to private data disclosed online. Now this has been done, and Article 17 has been discussed in chapters 3 and 4, some comments can be made with regards to both laws. A central drawback of the right to be forgotten as opposed to MPI is that it can't provide injunctive relief, as it is an *ex post* remedy – information it is invoked against may have already caused harm. In many circumstances, when erasure is quested under the right to be forgotten, the data in question will already be accessible online – so the information, to an extent, has already been disclosed. This is opposed to MPI, where if an injunction is granted by the courts before a story has gone to press or information has been otherwise released, then the public may never know the private information at all. However, injunctions are but one of the remedies available in MPI – damages being the other which only monetarily compensate a claimant on misuse of their data. In terms of efficiency, it is likely to be easier for a claimant to go to a website (particularly a large conglomerate such as Facebook) to request data's deletion or a national Data Protection Authority as opposed to mounting a lengthy, expensive MPI case which would involve hiring lawyers while *attempting* to obtain an interim injunction – and if this is granted, then awaiting a lengthy trial with the

[1090] Phillipson above, n 997.

expectation that the injunction is maintained. Even if an injunction is maintained, the problems of jurisdiction and dissent remain (as discussed above). One also cannot ignore statistics; few injunctions in MPI have been awarded in recent years despite the doubtlessly wide dissemination of private information online. The Ministry of Justice provides statistics for new injunctions awarded up until 2014: between January to June 2013 six injunctions were granted in MPI by the courts. That year between July and December no injunctions were awarded, and no injunctions were granted between January to June 2014.[1091] That equates to six injunctions over a three-year period; an inconsequential number. This can be accounted for by the fact that obtaining an injunction is time consuming and costly, and the outcome of a trial tenuous due to erratic decision-making on the part of the courts. It must also be noted that under Article 17, a data subject can request deletion of their personal information from a secure database (outside of the public domain). The right to be forgotten according to the Data Protection Act 2018 may indeed provide a more cost-effective and accessible route to redress for data subjects.

Conclusion

A logical way to view the decision in *Campbell* is that it was decided in order to curb press freedom at a crucial time – the decision occurred in the mid-2000s when digital news media were beginning to gain ground. A further societal shift has now taken place: now *social* media has begun to pose new challenges that may render MPI significantly less useful or even out-dated.[1092] This rise in social media usage has created specific problems for claimants seeking to rely on the tort. The doctrine of waiver may mean that if a data subject has disclosed personal information about a certain 'zone' of their lives online in the past (which is now more likely than ever before), the courts could view them as partially 'waiving' their right to privacy in respect of other information within that zone. Secondly, the public domain doctrine can act to bar an action in the event that personal information at issue is already in the public sphere to a significant extent; this is increasingly likely due to the ease and speed of data dissemination online circa 2019. That point is obviously linked to the practical problem that a potential claimant may not become aware that her data has been misused for some time, and when or if she does may conclude that the extent of its dissemination might mean it would be viewed by a court as already in the public domain, so an action would be

[1091] Statistics Bulletin, Ministry of Justice (25 September 2014) accessible at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/358274/privacy-injunctions-statistics-january-june-2014.pdf (last accessed 13/8/19).
[1092] Rowbottom above, n 817 at 170.

value-less. Or she might conclude that her privacy is irretrievably lost, and no court action, even if successful, could restore it. Thirdly, in the event that a claimant is successful in securing an injunction, an injunction's ability to protect a claimant's data is limited due to its jurisdictional scope and difficulties arising in the identification of who has disclosed data on the web in the event that an injunction has been breached[1093] and in the case of celebrities, the problem of mass dissent. These problems are compounded by the at-times pro-speech approach to MPI actions by the English judiciary. A cause for positive outlook is the two recent decisions of *PJS* and (to a lesser degree) *Sir Cliff Richard*, which may point to a judicial move towards fairly balancing privacy and expression interests in the digital age; that is particularly the case regarding the comments of the Supreme Court in the former case noting the damaging effects of personal information as publicly disclosed. It is therefore concluded that MPI has a limited role in addressing the protection of private information online. Therefore, the right to erasure provides a far greater prospect of providing such protection, so long as some of the aspects of the tort discussed above are not read into its interpretation.

[1093] Although there is now the potential for an injunction to be issued against 'persons unknown' in light of the ruling in *AMP*, discussed above.

Chapter 6: Defamation and the dissemination of false and private information online

Introduction

This thesis operates on a central premise or 'problem'; that protection for personality rights for individuals with respect to their information online is inadequate. So far, this PhD has considered two areas of law and their ability to provide redress for this problem – the right to be forgotten and misuse of private information. Due to the nature of these two areas, the majority of this thesis has concerned the remedies that an individual could obtain in the event that private and *truthful* information concerning themselves is published online. However, a person's personality rights are not just affected by the dissemination of truthful personal data on the internet; they are also affected by the spread of *false* and private data online. In certain circumstances, the spread of false information can be more reputationally damaging. Indeed, inaccuracy of information was a prime ground for exercising data protection rights under the 1995 Directive, as discussed in the case of *Google Spain* referred to in chapter 3. As this thesis has sought to demonstrate, when private, truthful material with the potential to injure a subject's reputation is made available online, an appropriate route for redress is currently the tort of MPI as well as the new right to erasure.[1094] Another route to redress for this second scenario, when private and false information is disseminated, is the tort of defamation. This thesis seeks to give a comprehensive answer as to how protected personality rights are in the digital age – and it is important this alternative scenario is now addressed.

The crux of defamation is the making of a defamatory allegation about the plaintiff to a third party or parties; the test for such an allegation is laid out within *Sim v Stretch*, 'would the words tend to lower the claimant in the estimation of right–thinking members of society?'.[1095] If this test is satisfied alongside a 'serious harm' threshold introduced in 2013,[1096] an action in

[1094] See Chapters 3, 4 and 5 of this thesis. O'Callaghan has observed that there is debate around a cross-over between defamation and privacy with regards to privacy-protection for false and private information, which he calls 'false privacy'. See Patrick O'Callaghan, 'False Privacy and Information Games' (2013) 4(3) *Journal of European Tort Law* 282.

[1095] *Sim v Stretch* [1936] 2 All ER 1237. It is important to note that traditionally there have in fact been several tests for defamatory statements in English law, however Lord Atkin's above-quoted test in *Sim v Stretch* has emerged as the leading example. Other tests include: if a statement can leave the claimant exposed to 'ridicule, hatred and contempt' as in *Thorley v Lord Kerry* (1812) 4 Taunt 355, 3 Camp 214n and whether the publication means that the individual will be shunned and avoided – see *Youssoupoff v Metro Goldwyn Mayer* (1934) 50 TLR 581 as set out by David Howarth, *Textbook on Tort* (Butterworths 1995) 544.

[1096] Section 1 Defamation Act 2013.

defamation will succeed,[1097] subject to any successful defence being raised. Defamation's central goal is to protect individual dignity at the expense of unrestricted expression. Crucially, defamation only protects against the publication of false information, truth[1098] being a complete defence to the action. This chapter will evaluate how recent reforms to the English law of defamation[1099] have helped or hindered data subjects seeking to initiate such an action against defamatory content online. As stated in the introduction to this thesis, this issue is of particular concern because the increasing prevalence of social media has resulted in the ability of defamatory allegations which are both false and personal to spread rapidly online,[1100] due to ease of republication and a vast potential audience.

The analysis of this chapter will form two main strands. Firstly, it will consider the stance of the European Court of Human Rights with regards to reputation and the protection of private life under Article 8, which it balances against freedom of expression under Article 10. This caselaw is of relevance to English defamation law due to obligations imposed on the English courts by the Human Rights Act 1998. Under section 3 of the Act, the English courts have an interpretive duty with regards to domestic law, the Act stating:

> 'So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights.'[1101]

This attempts to ensure it is in accordance with Convention rights including Article 10. Furthermore, under section 6 of the Human Rights Act the courts must act compatibly with the Convention rights as they are a public authority.[1102] It is necessary to consider some additional ECtHR caselaw in this chapter specifically on defamation, as these judgments have not been discussed in chapter 3 of this thesis. However, the normative framework sketched in chapters 3 and 4 still stands with regards to the analysis undertaken in this chapter, and the

[1097] This is a simplified summary of the decision procedure – a claimant must also not fall foul of one of the many defences available to defendants in defamation. Again, these defences will be considered in detail later in this section.
[1098] The 'truth defence', formerly known as justification, has been codified into statute in the Defamation Act 2013, section 2.
[1099] In other words, the Defamation Act 2013.
[1100] For example, social networking site Twitter allows a 'retweet' function which allows users to send another's tweet to their own followers. In the case of *Monroe v Hopkins* [2017] EWHC 433 (QB), [2017] W.L.R 68, several 'tweets' of the defendant (a relatively minor celebrity) were estimated by the court to have been seen by tens of thousands over just the period of a few hours.
[1101] Human Rights Act, section 3(1).
[1102] See the Human Rights Act 1998, sections 3 and 6.

balancing exercise that must be conducted in defamation actions (as well of those in MPI and right to be forgotten claims) between Article 8 and Article 10 rights.

Specific inadequacies of the reforms introduced by the Defamation Act 2013 will then be critiqued. The chapter next considers whether the codified defences of 'honest opinion' and 'publication on a matter of public interest'[1103] now offer greater clarity as well as an appropriate balance between reputation rights and freedom of expression. The focus of the second half of this chapter will be section 5[1104] of the Defamation Act which offers some redress for claimants who have been defamed on the web and the liability imposed on host websites. The 'single publication rule' and its potential to limit actions against republication of defamatory content online will also be briefly considered in this chapter.[1105] The analysis here as a whole will make reference to both English and Strasbourg jurisprudence, comparing the ECtHR's position with the English standpoint. A choice has been made here to omit certain sections of the 2013 Act from discussion – in particular, sections 1 the serious harm requirement in the Act and section 2, the truth defence.[1106] This is because the purpose of this chapter is not to give an overview of the 2013 Act. Rather, it is to make an argument that defamation law with respect to defamatory content online can act to bar redress for claimants due to the way common law has developed in this area, alongside aspects of the 2013 Act's drafting. It was felt that no significant (or *potentially* significant) change had been affected by the 2013 Act in respect of section 1[1107] and 2 of the Act versus the previous common law

[1103] Sections 3 and 4 respectively.
[1104] And the Defamation (Operators of Websites) Regulations 2013 made under it.
[1105] Section 8, Defamation Act 2013, if the information is in 'substantially the same form'.
[1106] Other omissions than these two sections have been made – such as the abolition (in large part) of jury trials in the Act.
[1107] Section 1 of the Defamation Act 2013 introduced what appeared to be additional hurdle to be overcome by claimants when seeking to mount an action in defamation: a 'serious harm' threshold. According to section 1(1), an individual must prove that a publication 'has caused or is likely to cause serious harm' to their reputation in order for material to be actionable. Three years before the new Act, in *Thornton v Telegraph Media Group Ltd (No.2)* [2010] EWHC 1414 (QB); [2010] EMLR 25, Mr Justice Tugendhat ruled that a court must apply a *threshold of seriousness* to exclude trivial claims when adjudicating upon defamation [50], so it was unclear whether section 1 raised the bar as to this threshold or maintained it. The following cases of *Cooke v MGN Ltd* [2014] EWHC 2831 (QB) and *Ames & Another v Spamhaus Project Ltd & Another* [2015] EWHC 127 (QB) confirmed that the bar had been raised 'modestly' from what it was prior to section 1's enactment (see *Cooke* [38]). The Court of Appeal's decision in *Lachaux v Independent Print Ltd* [2017] EWCA Civ 1334 endorsed the above position and overturned Mr Justice Warby's decision at trial that it was necessary to prove serious harm 'on the balance of probabilities'. See Iain Wilson and Tom Double, 'Business as usual? The Court of Appeal considers the threshold for bringing a libel claim in Lachaux v Independent Print Ltd' (*Inforrm*, 16 September 2016) accessible at: https://inforrm.org/2017/09/16/business-as-usual-the-court-of-appeal-considers-the-threshold-for-bringing-a-libel-claim-in-lachaux-v-independent-print-ltd-iain-wilson-and-tom-double/ (last accessed 28/4/18), Tom Bennett, 'Why So Serious? Lachaux and the threshold of serious harm in section 1 Defamation Act 2013' (2018) Journal of Media Law 1, 6 and *Lachaux v Independent Print Ltd* [2016] QB 402;

position – so focus has been placed on areas of the Act which are more problematic in terms of Article 8 (claimant) rights.

A. Data dissemination scenarios

This chapter, like others in this thesis, makes reference to the data dissemination scenarios present in this thesis' introduction. There is one such scenario which is of particular relevance – scenario VI, where an individual has been subject to online reports which are both false and reputationally damaging – the 'defamatory content' scenario. In order to give this chapter more depth and clarity, this scenario can be further broken down into yet more specific sets of circumstances:

i. Citizen journalist 'X' publishes online a news piece which discloses defamatory private information about person 'Y';

ii. A social networking site like Facebook hosts defamatory pieces or content posted by person Z about person Y;

iii. A website which has posted an article concerning a particular issue draws comments posted by third-party users which are defamatory about person Y;

iv. Person Z 'retweets' a defamatory piece concerning the private life of person Y.[1108]

B. Defamation at Strasbourg: reputation's protection under Article 8 ECHR

[2015] EWHC 2242. As this bar appears to only have been raised modestly, the decision was made to exclude analysis of this part of the Act from the chapter.

[1108] See social networking site Twitter's 'help centre': *'What is a Retweet?'*, accessible at: https://help.twitter.com/en/using-twitter/how-to-retweet (last accessed 2/2/18).

Several years after the passing of the Human Rights Act 1998 and for a short while prior, the English courts placed an emphasis on ensuring that the development and application of the law of libel was compatible with Article 10, the right to freedom of expression in the ECHR. Discussion of the competing right of reputation was given low priority in comparison.[1109] It should be noted at this point that the 'right to reputation' is a relatively young legal principle, and as such was consciously omitted from the text of Article 8 ECHR when the convention was drafted, only appearing as an interest which could restrict expression in the context of Article 10(2) ECHR. This prioritisation of expression is somewhat congruent to pre-2004 Strasbourg jurisprudence. In his dissent to the decision in *Lindon, Otchakovsky–Laurens*, Judge Loucaides observed that before the mid-2000s, the ECtHR's position was that reputation was not encompassed by Article 8, but rather to be treated as an exception to freedom of expression under Article 10(2). Judge Loucaides detailed the negative consequences of this approach:

> '…the case-law on the subject of freedom of speech has on occasion shown excessive sensitivity and granted over-protection in respect of interference with freedom of expression, as compared with interference with the right to reputation. Freedom of speech has been upheld as a value of primary importance which in many cases could *deprive deserving plaintiffs of an appropriate remedy for the protection of their dignity'.*[1110]

However, developments after 2004 signalled a change in attitude of the Strasbourg Court. Mullis and Scott believe this started with the recognition that reputation is protected by Article 8 in *Radio France v France*.[1111] When considering whether a legitimate aim was pursued by the French law of defamation, the court stated:

> 'The Court considers that the interference undoubtedly pursued one of the aims listed in Article 10 § 2, namely "protection of the reputation or rights of others"…The Court would observe that *the right to protection of one's reputation is of course one of the rights guaranteed by Article 8 of the Convention*, as one element of the right to

[1109] Alistair Mullis and Andrew Scott, 'The swing of the pendulum: reputation, expression and the recentering of English libel law' (2012) 61(3) *Northern Ireland Legal Quarterly* 27, 27, hereafter '*Mullis, Pendulum*'.
[1110] *Lindon* [emphasis added].
[1111] *Radio France v France* App no 53984/00 (ECHR, 30 March 2004) [31] and see *Mullis Pendulum*, 28.

respect for private life.'[1112]

However, despite this, the judgment in the case solely referenced Article 10 rights in deciding whether interference had been 'necessary in a democratic society', rather than a balancing exercise between Articles 8 and 10.[1113] There is no separate section of the judgment that considers factors of the case which relate to the strength of the Article 8 rights at issue. The Court took a strong position in *Pfeifer v Austria* three years later when it observed that if reputation was involved in a case, Article 8 would be engaged automatically.[1114] The Court commented that 'a person's reputation, *even if that person is criticised in the context of a public debate*, forms part of his or her personal identity and psychological integrity and therefore also falls within the scope of his or her "private life". Article 8 therefore applies.'[1115] This casts an undoubtedly wide net in respect of Article 8 rights.

Despite these developments, the ECtHR failed to explain what theoretical justification supported reputation being encompassed by Article 8. Alpin and Bosland suggest that the court may have had the personal dignity justification in mind, although any link between dignity and reputation had not been illuminated.[1116] The ECtHR finally addressed the issue, albeit briefly, in the case of *Karako v Hungary* in 2009:

> '…the Court reiterates that "private life" includes personal identity...The Court further observes that the Convention, as interpreted in the *Von Hannover* judgment regarding the individual's image, extends the protection of private life to the protection of personal integrity. This approach itself results from a broad interpretation of Article 8 to encompass notions of personal integrity and the free development of the personality.'[1117]

[1112] Ibid *Radio France* [31 – emphasis added].
[1113] Ibid [32-41].
[1114] *Pfeifer v Austria* App no 12556/03 (ECHR, 15 November 2007) [33-35].
[1115] Ibid [35].
[1116] Ibid and see *Chauvy and Ors v France* App no 64915/01 (ECHR, 29 June 2004), *Lindon* and Tanya Alpin and Jason Bosland,'The uncertain landscape of Article 8 of the ECHR: the protection of reputation as a fundamental human right?' in Andrew Kenyon (Ed.) *Comparative Defamation and Privacy Law* (Cambridge University Press 2016) 276.
[1117] *Karako v Hungary* App no 39311/05 (ECHR, 28 April 2009) [21].

In essence, the Court stated that the protection of reputation is important because of the harm caused by a particular presentation of a person's character to the autonomous development of their own personality.[1118] The Court found that *Von Hannover v Germany* extended the protection of Article 8 rights 'to the protection of personal integrity'.[1119] A further turning point arose out of *Karako* alongside *A v Norway* in 2009: both state that a threshold of seriousness has to be met in order for damage to reputation to engage Article 8.[1120] The Court in *Karako* noted that Article 8 would only be engaged by reputational harm in circumstances where:

> '…factual allegations were of such a *seriously offensive nature* that their publication had an inevitable direct effect on the applicant's private life…the applicant has not shown that the publication in question, allegedly affecting his reputation, constituted such a serious interference with his private life as to undermine his personal integrity.'[1121]

In *Karako* the Court reasoned that losing one's reputation does not always mean that personal integrity has been damaged – and only when personal integrity has been affected will Article 8 be engaged.[1122] *Karako* stated that reputation had 'only been deemed to be an independent right sporadically' under Article 8.[1123] *Axel Springer* in 2012 did not succeed in clarifying this situation; here the ECtHR made little comment on this threshold test and did not discuss the theoretical underpinnings of defamation law.[1124] The judgment did, however, note that the degree of 'seriousness' of the defamation concerned would have an impact in a case of whether member state defamation law unlawfully infringed Article 10 rights. In a paragraph entitled 'Limits on the freedom of expression' the Court observed:

> 'Article 10 § 2 of the Convention states that freedom of expression carries with it "duties and responsibilities", which also apply to the media…Thus, special grounds are required before the media can be dispensed from their ordinary obligation to

[1118] Ibid [21-23].
[1119] Ibid [21].
[1120] Alpin and Bosland above, n 1116 at 276-277. *Karako* above, n 1117 and *A v Norway* App no 28070/06 (ECHR, 9 April 2009).
[1121] Ibid *Karako* [23 – emphasis added].
[1122] Ibid *Karako* [23].
[1123] Ibid *Karako* [23] and also see Ian Helme, 'Cases - Karako v Hungrary', (*OneBrickCourt.com)* accessible at https://www.onebrickcourt.com/cases.aspx?menu=main&pageid=42&caseid=212 (last accessed 7/10/2017).
[1124] *Axel Springer*.

> verify factual statements that are defamatory of private individuals. Whether such grounds exist depends in particular on the *nature and degree of the defamation*…'[1125]

This approach seems more reminiscent of that in *Karako* (in its more limited application of reputation rights) than that in *Pfeifer* which advocated the universal application of Article 8 to defamation actions. In 2013, the case of *Ageyevy v Russia* was heard which concerned actions that spanned both privacy and defamation regarding reportage concerning a foster family's treatment of an adopted son.[1126] It was held by the Court that Article 8 was engaged as the family's reputation had been attacked in the articles (amongst other reasons); however, the pieces ran extreme headlines and contained emotive statements such as "Mummy with a devil's heart", so any threshold of seriousness implicitly employed by the courts would no doubt have been met by this content.[1127] More recently, in 2017, the ECtHR heard the case of *Einarsson v Iceland*, which concerned a defamation action which had been pursued in the Icelandic courts by an actor who was active on social media and generally in the public eye.[1128] In the case, person X had published a doctored photograph of said actor to a public Instagram page, writing 'loser' on the picture of the actor's forehead and emblazoned with the statement, 'fuck you rapist bastard.'[1129] This related to two accusations of rape which had been brought against the actor, both cases having been dismissed by an Icelandic public prosecutor through lack of evidence.[1130] The actor brought an action in defamation against person X, however a District Court in Iceland found against him – and subsequently, the Supreme Court in Iceland upheld this decision.[1131] The ECtHR stressed that a balance must be struck between the actor's Article 8 rights and person X's rights to expression,[1132] and observed that 'private life' under Article 8 was a 'broad concept.'[1133] The Court then went on to reference *Axel Springer*, and stated:

> 'However, in order for Article 8 to come into play, the attack on personal honour and reputation *must attain a certain level of seriousness* and must have been carried out in

[1125] *Axel Springer* [82 – emphasis added].
[1126] *Ageyevy v Russia* App no 7075/10 (*ECHR*, 18 April 2013).
[1127] Ibid [227].
[1128] *Egill Einarsson v Iceland* App no 24703/15 (*ECHR*, 7 November 2017).
[1129] Ibid [8].
[1130] Ibid [6].
[1131] Ibid [15].
[1132] Ibid [31].
[1133] Ibid [33].

> a manner *causing prejudice to personal enjoyment* of the right to respect for private life…'[1134]

The Court did find that the actor's Article 8 rights were engaged, and had in fact been violated.[1135] In 2017, then, the ECtHR can be seen as following the approach in *Karako* and requiring that a threshold of seriousness is met in order to engage Article 8 rights in defamation cases. Indeed, a similar conclusion regarding this threshold of seriousness was also reached a year later in *Faludy-Kovács v. Hungary*.[1136] In addition, the court noted in 2018 that someone's 'honour' could be protected under the auspices of Article 8.[1137]

Therefore, it is concluded that Strasbourg's current position appears to be that a threshold of some degree of seriousness must be met with respect to reputational harm in order for a claimant to argue that their Article 8 rights have been engaged through defamation of character.[1138] This is despite what was stated by the Court in the decision of *Pfeifer;* as the judgments in *Pfeifer* and *Karako* seemingly contradict each other, it appears that in light of *Einarsson* and *Faludy*, the 'threshold' test in *Karako* is the one that has won-out between the two approaches.

C. The inadequacies of the Defamation Act 2013

The Defamation Act 2013 was introduced (at least partly) as a result of lobbying by the Libel Reform Campaign[1139] calling for pro-speech alterations to the common law of defamation. Its inception must also be seen in the context of the Human Rights Act 1998 and Article 10 ECHR.[1140] Although the accuracy of some of the claims made during the reform campaign can be questioned and criticised on their own terms - including the claim that English libel law was a 'global pariah' in its prioritisation of reputation[1141] – the campaign was ultimately

[1134] Ibid [34 - emphasis added].
[1135] Ibid [53].
[1136] See *Faludy-Kovács v. Hungary* App no 20487/13 (*ECHR*, 23 January 2018) [26].
[1137] In an unusual case – see *Vincent Del Campo v Spain* App no 25527/13 (*ECHR*, 6 November 2018).
[1138] Additionally, the concept of a threshold of seriousness for claims was incorporated into English law under the new reforms in section 1 of the Defamation Act 2013.
[1139] See The Libel Reform Campaign.org, available at: http://www.libelreform.org/ (last accessed 29/8/18).
[1140] Although it received Royal Assent in 1998.
[1141] See Gavin Phillipson, 'The "global pariah", the Defamation Bill and the Human Rights Act' (2012) 63(1) *Northern Ireland Legal Quarterly* 149, 155. Phillipson argues that *on the contrary* to the claim that English law was a 'pariah' globally with its stance towards defamation (which the House of Commons Select Committee on

successful in securing new legislation. The 2013 Act codified major aspects of defamation law, thus seeking to correct what was seen as the common law's tendency to prioritise reputational interests.[1142] Again, the accuracy of this standpoint can also be criticised. Barendt argues that many judgments in defamation cases emphasised the importance of expression, including the seminal judgment in *Reynolds v Times Newspapers* which introduced the defence of 'publication on a matter of public interest'.[1143] Other aspects of the existing law also upheld free speech interests. Firstly, in *Derbyshire County Council v Times Newspapers* the Court of Appeal held that governmental bodies were unable to sue, limiting defamation's scope.[1144] Secondly, a long-standing common law rule forbade the issuing of injunctions against defamatory material in most circumstances.[1145] Finally, truth was a complete defence alongside a range of other available defences such as 'fair comment'.[1146] Despite these safeguards for expression, during the reform debates little attention was paid to the competing importance of personality rights.[1147]

Perhaps unsurprisingly, some members of the judiciary (particularly those adjudicating at first instance) are reticent to acknowledge that the law has changed in a substantial way. For example, the 2014 case of *Yeo* concerned a newspaper article regarding the lobbying of an MP by a private company.[1148] The issue turned on whether any of the three now statutory defences of truth, honest opinion or publication on a matter of public interest applied.[1149] The judge commented before his assessment:

> 'I have described the issues, and I shall resolve them, by reference to the common law…Online publication continued after 1 January 2014, when these common law defences were abolished and replaced by statutory defences under ss 2 to 4 of the Defamation Act 2013. Those defences are accordingly pleaded but, although I shall

---

Media Culture and Sport as well as former MP Nick Clegg suggested), English law set a global example, particularly for Commonwealth nations.

[1142] Ibid, 161.

[1143] *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127 - although it is important to note that this defence also encompassed a need of the publisher to verify the truthfulness of allegations.

[1144] Phillipson above, n 1141 at 155 and *Derbyshire County Council v Times Newspapers* [1992] 1 QB 770. This decision was also upheld in the House of Lords on appeal in the case.

[1145] Ibid.

[1146] As well as absolute and qualified privilege. Eric Barendt, 'Balancing Freedom of Expression and the Right to Reputation: Reflection on Reynolds and Reportage' (2012) 63(1) *Northern Ireland Legal Quarterly* 59, 60-61 and *Derbyshire County Council v Times Newspapers and others* (1993) HL 18 Feb 1993.

[1147] Phillipson above, n 1141 at 155.

[1148] *Yeo MP v Times Newspapers* [2014] EWHC 2853 (QB).

[1149] Now enshrined within sections 2,3 and 4 of the Defamation Act 2013, respectively.

> refer to some aspects of the new defences, *this will not be determinative*. *Neither side suggests, and I do not consider, that the 2013 Act altered the relevant law in any way that is material to the outcome of this case'.*[1150]

It will be argued in the next section of this chapter that, contrary to the view expressed in *Yeo*, there have been changes made to these defences by their codification into statute. Although the Explanatory Notes to the 2013 Act suggest that the new defences are to be interpreted in light of the common law, there are undoubtedly changes the textual wording of the provisions that alter the status quo.[1151]

I. A critique of the Defamation Act 2013, section 3: the statutory defence of honest opinion

i. Fair comment's codification into statute: 'honest opinion'

The defence of 'fair comment' at common law was the precursor to the 2013 Act's section 3 defence, named 'honest opinion'. The new Act abolished the common law fair comment defence and relevant legislation.[1152] The importance of the defence of fair comment has long been championed by the English courts, with the Report of the Committee on Defamation as long ago as 1975 labelling it 'a bulwark of free speech'.[1153]The defence at common law protected *honest expressions of opinion on matters of public interest*, and the judiciary had historically been keen to ensure that fair comment was generously interpreted in favour of a defendant. Lord Denning stressed this principle in *Slim v Daily Telegraph*:[1154]

> '…the right of fair comment is one of the essential elements which go to make up our freedom of speech. We must ever maintain this right intact. It must not be whittled down by legal refinements. When a citizen is troubled by things going wrong, he should be free to "write to the newspaper": and the newspaper should be free to

[1150] *Yeo MP v Times Newspapers* [2014] EWHC 2853 (QB), [29 – emphasis added].
[1151] Fair comment and the defence of 'publication in the public interest' are codified into sections 3 and 4 of the Act, respectively.
[1152] The Defamation Act 2013, section 3(8) – the piece of relevant legislation being section 6 of the Defamation Act 1952.
[1153] Report of the Committee on Defamation (Cmnd 5909, 1975) and see David Howarth, *Textbook on Tort* (Butterworths 1995) 571.
[1154] *Slim and others v Daily Telegraph Ltd and others* [1968] 2 W.L.R 599, 5 QB 157.

> publish his letter'.[1155]

Howarth explains the crucial purpose of the defence:

> 'The reason for the importance of the defence of fair comment is…Most human conversation is not about facts but about opinions…If the only defence to libel were truth, vast amounts of ordinary every day talk would become unlawful…'[1156]

Descheemaeker argues that the defence continues to be concerned with commentary, rather than opinion – that it is designed to protect a deduction or a meaningful criticism devised by careful thought.[1157] He observes that 'honest reasoning' is the root of the defence, and that there is no injury caused to reputation by a comment which is not authoritative and to be taken on face value.[1158] This is supported by dicta in modern caselaw; Mr Justice Nicol in *Butt* stated that comment is a 'deduction' or a 'criticism'.[1159] This defence could well apply to defamatory content released about an individual under the *third party poster* data dissemination scenario as detailed in this thesis' introduction – individuals are unlikely to have released false and defamatory information about themselves.

Several conditions had to be satisfied in order for a defendant to rely upon fair comment: firstly, the comment had to be on a matter of public interest. This could include commenting upon people holding public office, matters affecting the public at large[1160] and comments concerning bodies that are under the public's scrutiny.[1161] Secondly, the statement had to be a *comment* (an opinion). This condition has been subject of academic and judicial scrutiny for a number of years – Horsey and Rackley have noted that there is a fine line between facts and opinions.[1162] The dividing line that the courts set under fair comment was that an opinion is *evaluative*.[1163] In this sense, the common law defence of fair comment was already expansive (prior to the 2013 Act) in that it contained a generous reading of what constitutes 'opinion'. In the case of *Singh*, the defendant described the British Chiropractic Association as 'happily'

[1155] Ibid [170].
[1156] See Howarth above n 1153 at 571.
[1157] Eric Descheemaeker, 'Mapping Defamation Defences' (2015) 78 *Modern Law Review* 641, 652-653.
[1158] Ibid, 654.
[1159] *Dr Salman Butt v Secretary of State for the Home Department* [2017] EWHC 2619 (QB) [16–17].
[1160] Eg. in the mass media – books, plays, television.
[1161] *Telnikoff v Matusevitch* [1992] 2 AC 343, [1992] UKHL 2.
[1162] Kirsty Horsey and Erika Rackley, *Tort Law* (OUP 2015) Part III.
[1163] *British Chiropractic Association v Singh* [2010] EWCA Civ 350; [2011] EMLR 1.

promoting 'bogus treatments' for which there was 'not a jot of evidence.'[1164] The Court of Appeal held this was a statement of opinion because it was a *value judgement* that there was no worthwhile evidence supporting the efficaciousness of the treatments.[1165] However, it could be easily argued that Singh's statement was a statement of fact that the Chiropractic Association knew their treatments were bogus. In this sense, the defence was certainly lenient.

Thirdly, the comment must be based on truthful facts, *which were in existence when the statement in question was published.*[1166] The judgment of *Cohen* in 1968 firmly expounded that relevant facts arising post-publication were not sufficient to satisfy this third criteria.[1167] Finally, the comment's basis in fact must have also been indicated within the comment. This is final criteria is significant, as one of the reasons that fair comment is considered less damaging than false allegations of fact is because a requirement of fair comment is to indicate the basis for the opinion – and this way, the person who the comment is communicated to can come to their own conclusions. Howarth has also noted that the purpose of a defendant demonstrating that a comment had a factual basis is to maintain fairness. He states: 'if the defendant has based his comments on allegations that are not true, for example of he has called the plaintiff dishonest because he thought that the plaintiff had been convicted of theft when the plaintiff has no such conviction, the comment cannot be fair.'[1168] The rationale behind the defence of fair comment (and honest opinion) is that honestly held *opinions* on objective facts should not be censored, as this is an important aspect of freedom of expression. In this sense, advocates of the defence believe that a right is in play which is more important that the protection of reputation.[1169] The crux of the defence and its individual elements is to protect expressions of opinion in the public interest – to encourage debate in society, which in turn links to the 'facilitation of democracy' freedom of expression theory.[1170]

The new defence of honest opinion is set out in section 3 of the Act:

[1164] Ibid.
[1165] Ibid.
[1166] *Cohen v Daily Telegraph* [1968] WLR 916.
[1167] Ibid.
[1168] Howarth above n 1153 at 575.
[1169] As discussed in chapter 4 of this thesis.
[1170] And the marketplace of ideas. This was discussed in chapter 4 of this thesis. This point was made by Professor Richard Mullender in his lectures on tort law at Newcastle Law School, 2013.

> ‘(1)It is a defence to an action for defamation for the defendant to show that the following conditions are met.
>
> (2)The first condition is that the statement complained of was a *statement of opinion*.
>
> (3)The second condition is that the statement complained of indicated, whether in general or specific terms, *the basis of the opinion*.
>
> (4)The third condition is that an honest person could have held the opinion on the basis of—
>
> > (a)any fact which existed at the time the statement complained of was published;
> >
> > (b)anything asserted to be a fact in a privileged statement published before the statement complained of.
>
> (5)The defence is defeated if the claimant shows that the defendant did not hold the opinion.’[1171]

Defendants may not rely on honest opinion if malice is shown, as according to section 3(5) of the 2013 Act the defence cannot stand if a claimant shows that the defendant did not in fact hold that opinion. It should be noted that a statement does not need to be on a matter of public interest in order to fall within the new defence – the first most notable change.[1172] To summarise the text above, there are three main stages of the section 3 defence that now need to be satisfied for it to be relied upon: firstly, that the defamatory statement is one of opinion, secondly, that the statement indicates the basis of that opinion and thirdly, an honest person could have held that opinion on the basis of true facts (or privileged statements including statements that are in fact false but protected under section 4 of the Act).[1173]

The first condition of the section 3 defence (in subsection (2)) is that the comment must be a statement of *opinion* about facts, rather than a statement of fact. This mirrors the same requirement for fair comment and remains problematic for claimants for the reason explained above – the tenuous distinction that has been made (in certain cases such as *Singh*) by the courts between fact and opinion. Indeed, this position with regards to the differentiation

[1171] Defamation Act 2013.
[1172] As this is not a requirement present within section 3 of the Defamation Act 2013.
[1173] Defamation Act 2013 section 3, subsections (2), (3) and (4) respectively. This final point will be discussed in more detail later in this chapter.

between fact and opinion has remained consistent since the defence's reform, which has been shown by the 2019 Court of Appeal decision of *Butt.*[1174] Dr Butt edited a website called Islam21C which had been referred to in a government Press Release about Prevent, part of the UK's counter-terrorism strategy. At trial, Dr Butt argued that the statement in question regarding his website meant that he intended to radicalise people and preached hate.[1175] At first instance Lord Justice Nicol agreed with Dr Butt with regards to the ordinary meaning of the words but found that the Secretary of State had a defence in honest opinion as the statement was a statement of opinion, not fact.[1176] The Court of Appeal agreed with the trial judge on both of these issues, and the matter in contention was whether the statement was fact or opinion. Rowe states of the decision:

> 'As stated by the Court of Appeal, the test to be applied when determining whether a statement constitutes fact or opinion is "how the statement would strike the ordinary reader"…[1177] The Court was of the view that the ordinary reader would understand the statement about Butt in the press release to be a "highly value-laden", evaluative one…[1178] as opposed to an inferential statement of fact…'

The judgment stated that when deciding whether words constitute a statement of fact or opinion, courts will have to consider three things: subject matter, nature of allegation, context.[1179] In this respect, the defence has changed little from its prior position with regards to fair comment, [1180] in that value-statements will often be found to be opinions.

Section 3(3) has remained broadly the same as its common law predecessor in that the basis of the opinion has to be stated in 'general or specific terms'. The recent judgment of *Butt* has observed that this is in line with the common law position as set out in *Joseph v Spiller*:

> 'As Lord Phillips said in *Joseph v Spiller* at [94] it was sufficient "where the comment identified the subject matter of the comment generically as a class of material that was

[1174] *Dr Salman Butt v The Secretary of State for the Home Department* [2019] EWCA Civ 933.
[1175] Samuel Rowe, 'Case Law: Butt v Home Secretary, Honest Opinion Defence Clarified' (*Inforrm*, 10 July 2019) accessible at: https://inforrm.org/2019/07/10/case-law-butt-v-home-secretary-honest-opinion-defence-clarified-samuel-rowe/ (last accessed 22/8/19).
[1176] Ibid.
[1177] *Butt* above n 1174 [38].
[1178] Ibid [49].
[1179] Ibid [39] and Rowe above n 1175.
[1180] Rowe above n 1175.

> in the public domain. There was *no need for the commentator to spell out the specific parts of that material* that had given rise to the comment."'[1181]

Section 3(4) of the defence sets out the third condition: 'that an honest person could have held the opinion on the basis of…any fact *which existed at the time* the statement complained of was published' or anything 'asserted to be fact in a privileged statement'.[1182] The existence of an objective fact on which the opinion is based was also a condition which had to be satisfied under the common law defence of fair comment. Phillipson has observed that this position is harmonious with Strasbourg jurisprudence – the ECtHR in defamation caselaw has stated that such opinions need to be based upon pre-existing facts in cases such as *Dyuldin v Russia*.[1183] To come to such an opinion from the facts may be reasonable or unreasonable at common law; the requirement is that the opinion be 'one which could have been made by an honest person, however prejudiced he might be, and however exaggerated or obstinate his views'.[1184]

This requirement under fair comment also stressed the importance of a defendant honestly forming such an opinion on the basis of something *she had read*: Lord Denning said in *Slim* 'The writer must *get his facts right*: and he must honestly state his real opinion. But that being done, both he and the newspaper should be clear of any liability. They should not be deterred by fear of libel actions.'[1185] However, this aspect of the section 3 defence is different from its common law predecessor – and it is argued that it has been broadened to reflect a more 'pro-defendant' (or pro-expression) stance.[1186] The defence has shifted to become almost wholly objective in terms of contemporaneously existing facts, rather than a focus being placed only on facts that a defendant was *actually aware of* at the time they made the comment. This is evidenced by section 3(4):

> '4)The third condition is that an honest person could have held the opinion on the basis of—

[1181] *Butt* above n 1174 at [24–25].
[1182] Defamation Act 2013.
[1183] Phillipson above, n 1141 at 174 and *Dyuldin and Kislov v. Russia*, App no 5968/02 (ECHR, 31 July 2007).
[1184] *Tse Wai Chun Paul v Albert Cheng* [2001] EMLR 777.
[1185] *Slim* above, n 1154 [170].
[1186] Which is probably not surprising given the fact that the reforms were initiated to strengthen expression rights, as discussed earlier in this thesis.

> (a)any fact which *existed at the time* the statement complained of was published…'[1187]

According to this section, as long as such a supporting fact (giving rise to an opinion) existed at the time of the defamatory statement's publication, then this condition is satisfied – regardless of whether the defendant was aware of it or not. In practice, this could mean that a defendant, who has published an opinion on the basis of wholly false information (or indeed no facts or information at all) could succeed in relying upon the defence at trial if she is able subsequently to discover some fact that could be seen to support the opinion of which she was ignorant at the time she disseminated the defamatory opinion.[1188]

Therefore if a claimant attempts to pursue a claim relating to defamatory statements online, it will now be easier for a defendant to attempt to adduce a defence based on honest opinion, due to the now objective test present in section 3(4) for adducing existing facts giving rise to the statement. As well as providing multiple opportunities to defame individuals, the internet also provides a powerful resource as a researching tool. A plethora of factual information about various individuals is accessible through a simple Google search. It must be noted that their ability to find such a fact *ex post facto* would depend upon how specific their defamatory comment was, and how much content concerning the person is available in the public domain. For example, if the comment concerned a famous person, it would be more likely that such a fact would be found – as more material about their life would be reported in the media. Therefore, a defendant could possibly find and adduce a supporting fact (from the time they made the complained-of statement) at the time of trial, as there is now no requirement that the defendant had to in fact be aware of the fact *at that time*. Although the potential for a defendant to do this may be small, it is argued here that this avenue ought not to be open to defendants at all – and this is a result of the poor drafting of the 2013 Act.

Another aspect of the new defence's expansion is that the 'opinion' or statement at issue does not have to relate to a matter of public interest, which at common law was previously a requirement (as stated above).[1189] Now that this part of the defence has been removed, this will mean that the defence can theoretically be applied to expressions of opinion about

[1187] The Defamation Act 2013, section 3(4) [emphasis added].
[1188] Alastair Mullis and Andrew Scott, 'Tilting at Windmills: the Defamation Act 2013' (2014) 77(1) *Modern Law Review* 87. Hereafter '*Mullis Windmills*'.
[1189] Ibid. No public interest requirement is contained within The Defamation Act 2013, section 3.

people's purely private lives. Section 3 therefore has the potential to quash a multitude of potential claims concerning speech with little or no genuine public interest value, unduly restricting competing personality rights. Indeed, the presence of 'public interest' is relied upon as a touchstone to weigh freedom of expression interests against personality rights in the English and Strasbourg courts.[1190] This development can also be criticised on its own terms: if the purpose of all actionable defences to defamation claims is to uphold the importance of freedom of expression, then it would seem logical for the speech that a defence protects to have some value. By reference to freedom of expression's three main theoretical justifications – the pursuit of truth, the facilitation of democracy and personal autonomy – it is hard to see which of these justifications the publication of speech relating to purely private lives helps pursue.[1191] Furthermore, modern English jurisprudence has restated the importance of ranking the value of speech when it conflicts with personality rights in the widely discussed judgment of *PJS*,[1192] where Lord Mance stated that personal information about private lives was at the 'bottom end of the spectrum of importance', and therefore less deserving of expression-related protection.[1193] It appears that this alteration of the fair comment/honest opinion defence will enable it encompass the expression of opinions in this lowly ranking.

To summarise, the statutory defence of honest opinion's lack of a public interest requirement and its objective test for adduced facts within section 3(4) (meaning that a *defendant does not in fact have to been aware* of the facts they adduce in support of the statement) means that it will be more difficult for an individual to successfully claim in defamation with respect to any of the above four data dissemination scenarios – particularly scenario iii, which seems the most relevant; where 'a website which has posted an article concerning a particular issue draws comments posted by third-party users which are defamatory about person Y'. Problematic aspects of the old common law defence of fair comment also live on within section 3, including the troubled distinction between facts and opinions which has not been given any more clarity, as demonstrated in *Butt*.

ii. Overlap between section 3(4)(b) in honest opinion and the section 4 defence

[1190] See chapter 4.
[1191] Ibid.
[1192] *PJS*.
[1193] *PJS* [24].

Section 3(4)(b) states:

‘(4)The third condition is that an honest person could have held the opinion on the basis of—

…(b)anything asserted to be a fact in a privileged statement published before the statement complained of.’[1194]

Section 4(7) goes on to state:

‘(7)For the purposes of subsection (4)(b) a statement is a “privileged statement” if the person responsible for its publication would have one or more of the following defences if an action for defamation were brought in respect of it—

(a)a defence under section 4 (publication on matter of public interest)’[1195]

This means that in order to satisfy the ‘basis in fact’ condition within honest opinion, a defendant could rely on information presented to be fact in a ‘privileged statement’ according to section 3(4)(b).[1196] Section 4(7)(a) notes that such a privileged statement can include a publication that would be able to rely on the section 4 defence of publication on a matter of public interest.[1197] In essence, a defendant can successfully rely on the honest opinion defence by adducing a ‘publication on a matter of public interest’ as per section 4 to support the formation of their opinion, as it is a ‘privileged statement’. This is the case despite the fact that the ‘factual content’ within this publication is false; indeed, this is why the publisher of the privileged statement needed to rely on a section 4 defence, as detailed in section 4(7)(a). The result of this interchange is that the defence of honest opinion has been expanded due to a defendant’s ability to rely on ‘erroneous facts’[1198] due to this interaction between section 3 and section 4.

[1194] Ibid.
[1195] Ibid.
[1196] Ibid.
[1197] Ibid.
[1198] *Mullis Windmills*, 93.

This crossover is both problematic and complex; it enables a person to use defamatory information protected by one defence (section 4) in order to shield a separate defamatory statement using a different defence (section 3). Therefore a defendant can rely on 'defence-inception'[1199] in order to satisfy the requirements of honest opinion rather than proving that their opinion is rooted in truthful facts. Mullis and Scott noted that at draft Bill stage, privileged statements under section 4 were not to be included within the defence of honest opinion.[1200] They also note the inconsistency in approach of the Act – section 3(4)(b) requires that such a privileged statement - including one protected by section 4 – be published *before* the defamatory comment at issue, excluding the possibility of contemporaneous publication. This is not the case regarding section 3(4)(a) (an opinion being held based on any fact which existed at the time, not including privileged statements).[1201] This is but another example of poor drafting on the part of the 2013 Act.

II. A critique of the Defamation Act 2013, section 4: the statutory defence of publication on a matter of public interest

i. The *Reynolds* defence

Section 4 of the Defamation Act 2013 is a statutory version of the 'Reynolds' defence at common law. The original defence was created in the 2001 case of *Reynolds v Times Newspapers*, in which a former Taoiseach sued *The Times* in defamation for an article which claimed that he had deliberately and dishonestly misled the Irish parliament.[1202] Lord Nicholls held that, in determining whether the publication was covered by qualified privilege (by virtue of being in the public interest), the courts should assess whether the publication was in accordance with the standard of responsible journalism.[1203] Lord Nicholls set out a list of ten factors to be considered in this assessment, including:

1. The seriousness of the allegation.

2. The nature of the information.

[1199] In other words, using one defence to support reliance another defence – in this case, section 4 as supporting a separate reliance upon section 3, concerning two different publications.
[1200] *Mullis Windmill*, 93.
[1201] Ibid 94.
[1202] *Reynolds* above, n 1143.
[1203] Ibid.

3. The source of the information.

4. The steps taken to verify the information.

5. The status of the information.

6. The urgency of the matter.

7. Whether comment was sought from the plaintiff.

8. Whether the article contained the plaintiff's side of the story.

9. The tone of the article.

10. The circumstances of the publication, including the timing.[1204]

In essence, the common law *Reynolds* defence protected a matter of genuine public interest, reported responsibly. This defence again is likely to engage the *third party poster* data dissemination scenario – as its purpose is chiefly to protect people breaking news stories about other individuals. The defence could potentially also act as a shield for defendants in data-leak scenario VI as outlined in the introduction; where *information has been revealed online about an individual which is false and reputationally damaging*.

With regards to the scope of the *Reynolds* privilege, dicta from English caselaw has been inconsistent. In 2006, *Jameel*[1205] attempted to give some clarity to the existing law and tipped the 'balance' of the defence yet further in favour of expression. The House of Lords here held that when assessing whether something is a publication on a matter of public interest, the context of the whole article must be taken into account rather than just the defamatory statement itself.[1206] This could be seen as a pro-defendant development as if a public interest could not be found in the defamatory imputation, then defendants would have a second chance to adduce some public interest value in the publication at large. Furthermore, Baroness Hale encouraged the 'natural development' of the defence, arguing that lower courts had taken an unduly narrow stance towards it. Indeed, in the case of *Lindon* at

[1204] Ibid. Lord Nicholls stressed that this list was not exhaustive.
[1205] *Jameel and Another v Wall Street Journal* [2006] UKHL 44; [2007] 1 AC 359.
[1206] Barendt above, n 1146 at 62.

Strasbourg two years later, Judge Loucaides noted that the *Reynolds* defence served to prioritise Article 10 interests.[1207] It is important to remember the potential for *Reynolds* to encroach upon Article 8 rights. Harm may still be done to a claimant's reputation due to a false statement that is defensible under *Reynolds*, which would be the case if (for example) a defamatory article about a claimant was in the public interest and well-researched.[1208]

Several years after the decision in *Jameel*, came the decisions in *Flood v Times Newspapers*.[1209]The cases concerned an article in *The Times* (published in print and online) which stated that a police officer (the claimant) was under investigation for accepting bribes. The articles named the police officer as Gary Flood and noted that his home had been raided in an investigation into the matter.[1210] Flood brought a claim in defamation against *The Times*. *The Times* sought to rely on the *Reynolds* defence, and claimed that 'in the circumstances the publication of the Article was in the public interest and its journalists acted responsibly in composing and publishing it.'[1211] In response to this, Flood argued that as time passed the 'circumstances changed' and new information came to light which no longer justified the *continued* publication (access to) the articles online – the investigation into Flood had not found any evidence which suggested that Flood had supplied information for bribes, and no criminal or disciplinary action was to be taken against him.[1212]

The court at first instance in *Flood* took a moderately conservative approach to the defence – Lord Justice Tugendhat held that the articles attracted the *Reynolds* defence but the online publication was *no longer protected* under *Reynolds* after *The Times* were informed that the investigation into Flood had found no evidence against him.[1213] He stated:

> '…different factors applied to the continuing website publication of the article complained of. After September 2007, the defendant knew that the allegations had been investigated and knew the outcome of that investigation. The status of the information had therefore changed for the worse. No further evidence adverse to the

[1207] *Lindon,* and *Mullis Pendulum*, 49.
[1208] *Mullis Pendulum,* 50. As this is one of the criteria for 'responsible reportage' under the defence.
[1209] *Flood v Times Newspapers* [2010] EWCA Civ 804, [2012] UKSC 11.
[1210] Ibid [3].
[1211] Ibid [6].
[1212] Ibid [14-15].
[1213] [2009] EWHC 2375 (QB) [H11.6].

> claimant's case had come to light, and the defendant could no longer maintain that the website publication included a fair representation of the claimant's case…'[1214]

The Times appealed, and the Court of Appeal held that it was *not* in the public interest to report details of the *allegations* against Flood. It was noted in the Court of Appeal's judgment:

> 'The article went much farther than merely reporting the fact that the police were investigating an allegation of corruption, because it set out the details of what had been alleged and referred to the fact that the allegations were said to be supported by a dossier. Part of the contents of the dossier were then described, including references it was said to contain to a series of payments made by ISC totalling £20,000 to a recipient [named as Flood].'[1215]

Therefore whether the journalism was responsible was considered in the case.[1216] The Court of Appeal found that the journalists at *The Times* had not taken enough steps to verify the truth of the allegations made against Flood, and as a result their appeal was dismissed.[1217]The Supreme Court, in a marked change of position from the former two decisions, allowed *The Times*' appeal, and found that the article was protected under the *Reynolds* defence, with Lord Phillips noting that the article in the case was of 'high public interest'[1218]and 'that interest lay not merely in the fact of police corruption, but in the nature of that corruption.'[1219] Lord Phillips went on to observe that each factor in Lord Nicholls' list of requirements in *Reynolds* was not intended to be used in every case,[1220] and the Court also noted the importance of balancing Article 8 and 10 rights;[1221] in other words, balancing the harm done to an individual through being defamed with the importance of making certain information public.[1222] The degree of difference in approach between the judge at trial and the appellate

[1214] Ibid.
[1215] *Flood v Times Newspapers* [2010] EWCA Civ 804, [2011] 1 W.L.R. 153, [99]. Square brackets added.
[1216] Ibid [101].
[1217] Ibid [103-5].
[1218] *Flood v Times Newspapers* [2012] UKSC 11 [68].
[1219] Ibid.
[1220] Ibid [75].
[1221] As Professor Richard Mullender noted in his 2013 lectures on defamation in Tort law, Newcastle Law School, Newcastle University.
[1222] *Flood* above, n 1218 at [98].

courts in *Flood* shows the degree of definitional uncertainty which surrounds the *Reynolds* defence, the judiciary's conception of it, and how broadly it can be applied.

ii. General comments concerning codification

The purpose of codifying this defence in the 2013 Act was to give it greater legal certainty[1223] alongside the more generalised aim of enhancing Article 10 rights.[1224] However, it could be argued that (to the contrary) section 4 lacks true reform. Caselaw relating to the common law *Reynolds* defence has *theoretically* been abolished under the new Act,[1225]so one would assume that Lord Nicholls' list of *Reynolds*-factors would now be obsolete. However, the explanatory notes to the Act detail – somewhat confusingly – that prior case law will be relevant and informative to how the new defence will be interpreted.[1226] In light of this, the question must be posed then whether the requirement of responsible journalism has actually been dispensed with, given the fact that Lord Nicholls' list relates to responsible reportage. It appears as if the courts, when seeking to adjudicate on the scope of the new defence, may be caught within a state of flux between the old defence and its new formulation, with the extent of their similarities unclear. As of yet, contemporary caselaw has not produced an alternative list to take the place of these factors. Howarth argues that in relation to the *Reynolds* defence at common law, it was difficult for judges to understand the activities of the press when adjudicating on the defence.[1227] There is also some concern with regards to the difficulties the judiciary may face in applying section 4, which contains even less guidance.[1228]

Section 4 of the Defamation Act reads as follows:

> '(1) It is a defence to an action for defamation for the defendant to show that—

[1223] As opposed to being governed by case-precedent (the common law). See *Mullis Windmill*.
[1224] Ibid.
[1225] The Defamation Act 2013, section 4(6).
[1226] Explanatory Notes to the Defamation Act 2013, Chapter 26, available at: http://www.legislation.gov.uk/ukpga/2013/26/pdfs/ukpgaen_20130026_en.pdf (last accessed 28/3/18) and see Phillipson above, n 1141.
[1227] David Howarth, 'Libel: Its purpose and Reform' (2011) 74(6) *Modern Law Review* 845, 871.
[1227] Defamation Act 2013.
[1228] Ibid.

(a)the statement complained of was, or formed part of, a statement on a matter of public interest; and

(b)the defendant reasonably believed that publishing the statement complained of was in the public interest.

(2) Subject to subsections (3) and (4), in determining whether the defendant has shown the matters mentioned in subsection (1), the court must have regard to all the circumstances of the case.

(3) If the statement complained of was, or formed part of, an accurate and impartial account of a dispute to which the claimant was a party, the court must in determining whether it was reasonable for the defendant to believe that publishing the statement was in the public interest disregard any omission of the defendant to take steps to verify the truth of the imputation conveyed by it.

(4) In determining whether it was reasonable for the defendant to believe that publishing the statement complained of was in the public interest, the court must make such allowance for editorial judgement as it considers appropriate.

(5) For the avoidance of doubt, the defence under this section may be relied upon irrespective of whether the statement complained of is a statement of fact or a statement of opinion.

(6) The common law defence known as the Reynolds defence is abolished'[1229]

In essence, in order to rely on the defence, the statement must be on a matter of public interest and a defendant must reasonably believe that the publication of the statement was in

[1229] Defamation Act 2013.

the public interest.[1230] In establishing the latter requirement, the court must take into account 'editorial judgement'[1231] and the defence also covers the neutral reportage of litigation[1232] and statements of opinion,[1233] leading to an intersection between section 4 and the section 3 defence of honest opinion.[1234]

iii. Section 4(1): public interest and reasonable belief

As noted above, section 4(1)(a) and (b) state that to successfully rely on the defence that the defendant must show:

'(a) that the statement concerned is a matter in the *public interest* and
(b) that they *reasonably believed that the publication of the statement was also in the public interest*.'

A wide reading of reasonable belief here would mean that the defence would only fail (on these grounds) if the belief was proven false, capricious or irrational.[1235] Such a reading would potentially breach Article 8 rights; to prove a belief was irrational would be an extremely high threshold for a claimant to reach. Scott and Mullis note that a narrow interpretation of section 4(1)(b) could be that a responsible journalist following ethical procedures would generate a reasonable belief.[1236] This is in keeping with the common law *Reynolds* defence, which protected responsible reportage. The authors argue that this second formulation was the intention of parliament when drafting the legislation.[1237] While this may be the case, the possibility of an alternate or broader reading is a cause for concern for advocates of reputation, or Article 8 rights – particularly as section 4 is overshadowed by an overwhelming lack of clarity, making an alternative interpretation possible. It is important to note that it is unlikely that an unduly broad interpretation would be adopted due to the

[1230] Section 4 (1) (a) and (b) of the Defamation Act 2013.
[1231] Section 4(4) Defamation Act 2013.
[1232] Section 4(3) Defamation Act 2013.
[1233] Section 4(5) Defamation Act 2013.
[1234] This interaction between sections 3 and 4 of the Defamation Act 2013 will be elaborated upon on later this chapter.
[1235] *Mullis Windmill.*
[1236] Ibid.
[1237] Ibid.

application of section 3 of the Human Rights Act which requires courts to ensure that legislation is interpreted compatible with ECHR rights – including Article 8.[1238]

As of yet, only a small amount of caselaw considering the new section 4 defence is available. However, some tentative observations can be made. In at least two judgments the courts have interpreted section 4's requirement of 'reasonable belief' [that the publication is in the public interest] to relate to the *overall importance* of the publication rather than just a belief in that the *subject matter of the publication itself* is public interest-worthy.[1239] The 2017 judgment in *Malkiewicz* quoting the earlier decision of *Economou* stated of section 4(2) that:

> 'To satisfy this second requirement, which I shall call "the Reasonable Belief requirement", the defendant must (a) prove as a fact that he believed *that publishing the statement complained of was in the public interest,* and (b) persuade the court that this was a reasonable belief.'[1240]

This position is congruent with *Jameel*[1241] as earlier discussed, and is perhaps an early indication that little may practically change with regards to the application of this defence in this respect.

Section 4(2) and (4) requires the courts to assess the defendant's reasonable belief in the public interest in light of 'all the circumstances of the case' and make appropriate allowances for editorial judgement[1242]and so adopts a similar stance to that of the common law defence. By way of some early direction, the post-2013 case of *Economou* has stated that:

> '(4) The "circumstances" to be considered pursuant to s 4(2) are those that go to whether or not the belief was held, and whether or not it was reasonable.'[1243]

[1238] Gavin Phillipson, *Memorandum to the Joint Committee on Human Rights: the Defamation Bill 2012, Executive Summary*, BILLS (12-13) 066 – see page 9 onwards and *Mullis Windmill.*
[1239] See later in this chapter where this is discussed in detail.
[1240] *Economou v de Frietas* [2016] EWHC 1853 (QB) [139] and *Jan Tomasz Serafin v Grzegorz Malkiewicz, Czas Publishers Ltd, Teresa Bazarnik-Malkiewicz* [2017] EWHC 2992 (QB) [310 – emphasis added].
[1241] *Jameel* above, n 1205 and Barendt above, n 1146 at 62.
[1242] The Defamation Act 2013, section 4, emphasis added.
[1243] *Economou v de Frietas* [2016] EWHC 1853 (QB) [139].

In terms of what reasonable belief in fact *is, Economou* stated that this will be assessed on a highly context-dependent basis that concentrates on the statement and the statement-maker's state of mind.[1244]

The Joint Committee on the Draft Defamation Bill[1245] argued that the section 4 defence should take into account the *resources* of the publisher or author of the defamatory statement. This approach is contested here – aside from the fact that a large media company (such as the Mirror Group, who are frequently subject to actions in defamation and MPI) often have a vast amount of financial backing to support research, the resources of a publisher has no bearing upon the level of harm that a defamatory statement could inflict upon the social and mental wellbeing and reputation of a claimant.[1246] This approach would unfairly prioritise expression by allowing a potentially devastating defamatory claim that has been poorly investigated to be protected under the defence. Such a scenario could come about where, in a *third party poster* scenario, someone who is a 'lone wolf' internet user with little resources uploads personal data about another online which is both false and reputationally damaging (data-leak scenario VI, as per this thesis' introduction). Worryingly, in the leading Court of Appeal case on this issue subsequent to the 2013 Act – *Economou*[1247] – moves have been made towards adopting this approach. The facts of the case concerned the claimant, Economou, who had been falsely accused of rape by the since deceased daughter of de Freitas – before her death, the Crown Prosecution Services were preparing to mount a case against Ms. de Freitas for perverting the course of justice.[1248] Mr de Freitas had been advised by his legal team to give information to the press and he had done so – and the case turned on four newspaper articles and two BBC broadcasts.[1249] The claimant, Economou, brought an action against de Freitas. The case in general (as well as the earlier decision of the High Court in the matter) adopts an expansive reading of the section 4 defence. The salient point that emerges from the Court of Appeal's decision is that for the section 4 defence to apply, the article(s) in question do not

[1244] Ibid [161].
[1245] See for example the Joint Committee on the Draft Defamation Bill, Session 2010-2 (minutes), HL Paper 203, accessible at: https://publications.parliament.uk/pa/jt201012/jtselect/jtdefam/203/203.pdf (last accessed 3/9/18).
[1246] See Barendt above, n 1146 at 71 – who makes this claim with regards to the argument that pro – claimant leverage should be given to the defamatory reportage of citizen journalists online due to their lack of resources.
[1247] *Economou v de Frietas* [2018] EWCA Civ 2591.
[1248] Ibid [1-9].
[1249] Ibid and see Dominic Garner, 'Case Law: Economou v de Freitas, Court of Appeal guidance on "public interest" defence' (Inforrm, 5th December 2018) accessible at: https://inforrm.org/2018/12/05/case-law-economou-v-de-freitas-court-of-appeal-guidance-on-public-interest-defence-dominic-garner/ (last accessed 11/9/19).

necessarily have to be well-researched by the defendant. The High Court's decision (upheld by the Court of Appeal) widened the scope of the defence to incorporate 'contributors' to newspaper articles like Mr de Freitas who have no real journalistic role in conducting any legitimate research linked to the publication. The case has effectively created 'contributor immunity'[1250] under the auspices of the section 4 defence by allowing de Freitas to rely upon it, despite the fact that he had made serious (and false) allegations about the claimant on which several news articles were based. The decision to allow de Freitas to successfully rely on the defence was maintained by the Court of Appeal, regardless of the fact that de Freitas' conduct had fallen 'far short' of what would normally have been expected by a journalist seeking to rely on the *Reynolds* defence.[1251] This move on the part of the courts is concerning for a number of reasons: firstly, as the claimant in the case argued, it allows a person to embark on a 'media strategy' to defame by leaking false statements to the press – with the defamer then able to then seek protection under section 4.[1252]Secondly, it can be argued that not enough attention was paid by the courts to the severity of the information at issue here – the court adopted an expansive interpretation of the defence in a case which concerned *a rape allegation*, one of the most serious crimes a person can be accused of. These decision could be viewed as a concerning early warning-sign that the most senior courts in England and Wales are keen to adopt an expansive approach to the new section 4 defence.

The fact that what constitutes 'reasonable belief'[1253] is left partially subjective[1254] and unspecified within section 4 could also potentially lead to a pro-defendant bias, depending on its future interpretation. Indeed, there are early signs of this already emerging in the caselaw. The decision of *Economou* in the Court of Appeal was keen to emphasise that the section 4 defence was inherently flexible, and stress that a highly context-dependent approach to the defence ought to be adopted, focused on the defendant in question.[1255] In the instant case, it

[1250] Ibid Garner and *Economou* [2018] EWCA Civ 2591 at [107].
[1251] Ibid *Economou* [2018] EWCA Civ 2591 at [104].
[1252] Ibid [108] and Dominic Garner, 'Case Law: Economou v de Freitas, Court of Appeal guidance on "public interest" defence' (Inforrm, 5th December 2018) accessible at: https://inforrm.org/2018/12/05/case-law-economou-v-de-freitas-court-of-appeal-guidance-on-public-interest-defence-dominic-garner/ (last accessed 11/9/19).
[1253] Reasonable belief that the publication of the statement is in the public interest.
[1254] In the sense that the defendant must themselves reasonably believe that publication is in the public interest, according to section 4(1)(b) of the Act.
[1255] Dominic Garner, 'Case Law: Economou v de Freitas, Court of Appeal guidance on "public interest" defence' (*Inforrm*, 5 December 2018) accessible at: https://inforrm.org/2018/12/05/case-law-economou-v-de-freitas-court-of-appeal-guidance-on-public-interest-defence-dominic-garner/ (last accessed 11/9/19).

was deemed relevant that Ms. de Freitas was the defendant's primary or sole source of information (she had insisted to her farther that her rape claim against Economou was legitimate) and his belief was therefore reasonable; this demonstrates the subjective nature of the defence.[1256] His 'proximity' to the events of the case, the Court held, also made it reasonable.[1257]

If an undue amount of influence is placed upon what a defendant believed as a reporter, and the subjective aspect of the test emphasised, then a shift in a court's analysis may take place – from the harm done to a claimant[1258]to the mind of a defendant. This could potentially lead to an imbalance of reputational and expression interests in the sense that this could potentially result in the severity of the reputational damage being given a comparatively low priority in the analysis of the court (indeed, there are early signs of this in *Economou*), with only a reckless publisher being disallowed from relying upon section 4. In another recent case of *Doyle v Smith*, the court has demonstrated what it would deem a 'bridge too far' in terms of a defendant's reliance upon section 4.[1259] The case related to four local news articles which had been published that suggested that the claimant had been part of a ten million pound fraud scandal. The defendant's reliance on the section 4 defence here failed as he did not have reasonable belief according to section 4(1)(b) that the publication was in the public interest. The Court found that the claimant knew that at least some of the statements he made weren't true[1260] so there was no *belief* in the public interest value here – and even if there had been a belief in the public interest, the Court noted that it would not have been 'reasonable.'[1261] In this case then, the defence did not fail because the defendant was a reckless publisher – it failed because he was a deliberately dishonest one. Further to this, it must be noted that an *obvious* bias in favour of expression rights over reputational interests would be likely avoided by the courts, due to their obligations under section 3 of the Human Rights Act to interpret legislation compatibly with Convention rights of both Articles 8 and 10.[1262] However, this

[1256] *Economou v de Frietas* [2018] EWCA Civ 2591 [65 and 98] and *Economou v de Frietas* [2016] EWHC 1853 (QB) [249].
[1257] Dominic Garner, 'Case Law: Economou v de Freitas, Court of Appeal guidance on "public interest" defence' (*Inforrm*, 5 December 2018) accessible at: https://inforrm.org/2018/12/05/case-law-economou-v-de-freitas-court-of-appeal-guidance-on-public-interest-defence-dominic-garner/ (last accessed 11/9/19).
[1258] Which was still to some extent the focus of the Reynolds defence – Lord Nicholls' 'laundry list' of factors included the tone of the article and the severity of the accusation.
[1259] *Doyle v Smith* [2018] EWHC 2935 (QB).
[1260] Ibid [84].
[1261] Ibid [85]
[1262] Section 3, 'Interpretation of Legislation', Human Rights Act 1998.

does not mean that some subtle shift in priority may not occur, in particular because one purpose of the new Act was to reinstate the importance of expression.[1263]

A key problem with the text of section 4 is its lack of precision, which somewhat contradicts one of the purposes of codification – to give clarity. Crucially, what constitutes a matter of public interest is left undefined by the Act. This could potentially result in a pro-defendant bias, as a wide array of information could theoretically be argued to be of public interest. Indeed, English caselaw has been littered with varying approaches to the public interest with regards to the tort of MPI.[1264] At the very least, the notion of what constitutes the public interest could be reinterpreted[1265] from its prior common law definition in defamation. Lord Hoffmann in *Jameel* could be said to indicate the common law's approach to public interest (prior to the adoption of section 4), stating:

> 'the public tends to be interested in many things which are *not of the slightest* public interest.'[1266]

This appears to imply that some legitimate aspect of wider societal interest, aside from banal data about private lives, needs to be present within information to give it public interest value. Traditionally, several types of information have been considered to automatically attract the public interest: the official conduct of people in public office, the behaviour of government and public authorities and the organisation and running of institutions attracting public concern.[1267] A classic example of information which clearly involves the public interest was present in the case of *Radio France v France*, the Strasbourg court observing:

> 'There is no doubt that the attitude of senior French administrative officers during the Occupation is a question commanding the highest public interest and that the

[1263] *Mullis Windmill.*
[1264] A pro-defendant approach was evident in cases such as *Ferdinand* where it was deemed that private information about a footballer's lover was in the public interest to disclose, however a pro – claimant stance (and a narrowing of what constitutes the public interest) is evident in the more recent case of *PJS*, which considered that the value of speech, particularly when it concerns trivial gossip about a celebrity's private life should be properly assessed.
[1265] Phillipson above, n 1141 at 166.
[1266] *Jameel* above, n 1205 [49 – emphasis added].
[1267] Professor Richard Mullender helpfully observed in his 2013 lectures on defamation in tort law, Newcastle Law School, Newcastle University.

> broadcasting of information about it forms an integral part of the task allotted to the media in a democratic society.'[1268]

Aside from these entrenched examples, the periphery of what constitutes a matter of legitimate public interest remains contested in the English and Strasbourg courts, particularly regarding how this relates to information concerning private lives. Section 4 of the new Act does nothing to give clarity to this situation. Initial post-2013 caselaw has been subdued in its guidance as to what constitutes the public interest under section 4, choosing instead to focus on other aspects of the section 4 defence (in particular, reasonable belief). In *Economou*, the Court of Appeal found that the criteria was easily met considering the case concerned a rape allegation.[1269] The case of *Doyle* didn't take this issue much further, Mr Justice Warby noting that this was an objective question and referred to the well-trod suggestions made in the judgment of *Reynolds* (the public interest includes matters of election and public administration).[1270] Future caselaw may shed some light on this issue.

iv. Citizen journalists

An important issue to be considered in relation to section 4 as a whole is whether it can and should apply to citizen journalists online, as per scenario data scenario 'i' in this thesis where a 'citizen journalist', 'X' online publishes a news piece which discloses false private information about person 'Y'. A citizen journalist can be defined as loosely as any private individual who attempts some type of investigative or critical reportage online, which is somewhat of a 'catch-all' criteria. Phillipson has observed that the new defence has the potential to protect amateur journalists, as opposed to being confined to professionals.[1271] Indeed, the case of *Seaga v Harper* noted that the *Reynolds* defence applied 'beyond' traditional media five years before the new Act's introduction, and was intended to have a liberalising effect on the law.[1272] There are two issues that must be considered here: firstly, whether the doctrine of *neutral reportage*[1273] should be open to citizen journalists and

[1268] *Radio France* above, n 1111 [34].
[1269] *Economou v de Frietas* [2018] EWCA Civ 2591 [17].
[1270] *Doyle v Smith* [2018] EWHC 2935 (QB) [69].
[1271] Phillipson above, n 1141 at 170.
[1272] *Edward Seaga v Leslie Harper* [2008] UKPC 9. Also see Kate Wilson, 'Case Analysis – Edward Seaga v Leslie Harper [2008] UKPC 9', (*Onebrickcourt.com*) (last accessed 3/4/18) and Barendt above, n 1146 at 71.
[1273] Under the common law *Reynolds* defence, if a journalist had engaged in responsible journalism and reported facts about an allegation in a 'neutral' or balanced manner then defamatory content within an article would be protected. This has been codified within section 4(3) of the Defamation Act 2013.

secondly, whether a 'publication in the public interest' section 4 defence in general should apply to citizen journalists. They will now be dealt with in turn.

Collins has gone as far as to argue that a neutral reportage defence should not only be applied to citizen journalists, but this application should be administered with a degree of 'latitude'; requirements of the defence relaxed to account for a citizen journalist's lack of resources.[1274]This approach is strongly contested. As Barendt argues, this latitude fails to account for the fact that a person's reputation can be irrevocably damaged by virtue of single, poorly-researched 'report' online.[1275] Due to the fact that citizen journalists may have comparatively less financial resources than large media outlets, it is therefore more foreseeable on their part that their facts may be incorrect and defamatory – arguably, because of this a greater onus should be placed upon them to ensure that an inflammatory post is *least in part factually correct.*

Secondly, it is argued that section 4 as a whole should not be available as a defence to citizen journalists. It is clear from Lord Nicholls' factors that the extent to which an article is researched was intended to be a pivotal consideration in the success of the defence – four out of his ten factors relate to this issue, namely the factors of 'the source of the information', 'steps taken to identify the information', 'whether comment was sought from claimant' and 'whether the publication contained the claimant's side of the story'.[1276] This is a significant proportion of the list to dedicate to responsible publication, and was by no means incidental. The combination of these factors leads one to the conclusion that the better researched an article is, the more likely that a defendant could successfully rely upon the public interest defence. Hence, at least part of the reason for the inception of the common law defence was to protect journalists acting in a *professional manner* (be it online or offline) by engaging in responsible and thorough journalism when gathering and publishing pieces of information or allegations that are potentially defamatory. Many of those who could be considered citizen journalists online will not possess ethical or specialised journalism training, contrary to a career journalist. As stated above, to extend (what was formerly) the *Reynolds* defence in this way would mean that in theory anyone posting something false and defamatory online which

[1274] Barendt above, n 1146 at 71 and Matthew Collins, *The Law of Defamation and the Internet* (OUP 2001).
[1275] Ibid Barendt.
[1276] *Reynolds* above, n 1143.

was in some way related to the public interest could potentially be protected by it. If this is the case, then it is contested that section 4 would cease to be a genuine journalistic defence.

There has been varying indications by the courts as to the approach they will be adopting regarding section 4's application to citizen journalists. The trial judge in *Malkiewicz* stressed the importance of the *Reynolds* factor of *verifying* information:

> '…section 4 requires…that he, she or it took *reasonable steps to ascertain the reliability and credibility of the substantive content of the publication*. In other words, the publisher must undertake reasonable inquiries, come to a reasonable conclusion that any sources are reliable and credible, and, where appropriate, obtain the target's version before publication...'[1277]

This is a staunch restatement that Lord Nicholls' original factors relating to responsible publication still have crucial relevance to the success of the new section 4 defence, and could have been interpreted as a sign that the courts were not willing to extend the scope of the defence beyond the actions of trained, responsible journalists – however, the decisions in *Economou* seem to make it clear that the courts are in fact willing to encompass citizen journalists within section 4's protection. As discussed above, the decisions in the case effectively expanded the defence to give contributors to news articles containing defamatory statements immunity. The case (at both the High Court and the Court of Appeal) was decided using a highly context-dependent and fact-dependent approach to the defence which would favour citizen journalists. It seems clear from this extension of the defence to cover contributors (who are not required to do any research to rely on the defence) that it will be extended to cover citizen journalists too – who could potentially be allowed to rely on the defence despite the fact that have not conducted robust investigation into what they have published. Lady Justice Sharp noted that the defence did not merely apply to traditional journalism, stating:

> '…it is not necessary to expatiate on the importance of freedom of expression…The importance of the right in this arena is what led to the recognition of the Reynolds defence, and to the subsequent enactment of the public interest defence in section 4 of

[1277] *Malkiewicz* above, n 1240 [335 – emphasis added].

> the 2013 Act. This defence is *not confined to the media, which has resources and other support structures others do not have.* Section 4 requires the court to have regard to *all the circumstances of the case* when determining the all-important question arising under section 4(1)(b)…'[1278]

Indeed, the fact that Lady Justice Sharp went on to note that 'all the circumstance of the case' must be considered after suggesting that the defence lay open to the non-traditional media appears to suggest that not only will citizen journalists be able to rely on the defence, but their lack of resources for fact-checking information must also be taken into account. Garner has noted that in terms of the assessment in *Economou*, section 4 may now have 'bespoke' application to different types of journalists in different circumstances.[1279]It is argued here that this potential extension of section 4 to citizen journalists (as per data dissemination scenario i at the beginning of this chapter) is concerning – including citizen journalists who may have undertaken little or no research into the validity of their claims before publishing them online.

v. Will anything actually be different under section 4?

Despite the fact that this chapter has sought to argue that the new section 4 statutory codification of *Reynolds* has the potential to change the scope of the defence (with a pro-defendant bias), Descheemaeker has argued that the 2013 act has not fundamentally altered the defence.[1280] Indeed, the court in *Economou* also observed that the truth of the statement is not important as long as section 4(1) is satisfied, which was the status quo before the defence was codified.[1281] In addition, the early post-2013 case *Malkiewicz* stressed the importance of defendants verifying information for reliance upon the new section 4 defence – which was one of Lord Nicholls' original ten *Reynolds* 'factors' as discussed above.[1282] This, combined with the statement that all of the *Reynolds* factors are still relevant to section 4 (in the Act's Explanatory Notes), arguably shows that the judiciary will continue to some extent to look backwards in interpreting section 4. Further to this, despite the fact that certain aspects of the case in *Ecomomou* appeared to newly extend section 4's defence (with a more flexible

[1278] *Economou v de Frietas* [2018] EWCA Civ 2591, [110].
[1279] Dominic Garner, 'Case Law: Economou v de Freitas, Court of Appeal guidance on "public interest" defence' (*Inforrm*, 5 December 2018) accessible at: https://inforrm.org/2018/12/05/case-law-economou-v-de-freitas-court-of-appeal-guidance-on-public-interest-defence-dominic-garner/ (last accessed 11/9/19).
[1280] Descheemaeker above, n 1157.
[1281] *Economou v de Frietas* [2016] EWHC 1853 (QB) [139-140].
[1282] *Jan Tomasz Serafin v Grzegorz Malkiewicz, Czas Publishers Ltd, Teresa Bazarnik-Malkiewicz* [2017] EWHC 2992 (QB) [335].

approach towards defendants), other parts of the judicial reasoning in the decision relied heavily on caselaw prior to the 2013 Act – and in particular, *Reynolds*. [1283] Lady Justice Sharp in the case also noted that the rationales behind both the *Reynolds* defence and section 4 were 'not materially different'.[1284]

It cannot be denied that at least some of the changes that this chapter has discussed at length give the judiciary the *opportunity* to re-interpret the defence in a pro-defendant fashion, although whether this will happen in the long-term is unclear. It is submitted that a more defendant-friendly public interest defence is a step in the wrong direction; to the contrary, an emphasis on personality rights is needed in order to rebalance Articles 8 and 10 online. If the defence is reinterpreted broadly, it would be additionally difficult for a claimant to seek redress in a data-leak scenario where a *third party poster* uploads false and reputationally damaging content concerning them. It is important to remember the principle expounded within *Loutchansky*: the function of qualified privilege is to allow the publication of *important allegations* which cannot conclusively to be shown to be true, as withholding such information would be detrimental to the public interest.[1285] When interpreting section 4 in relation to online disclosures, the judiciary must carefully consider what constitutes an 'important allegation' – this is due to the significant reputational harm that can be caused to a claimant through such a disclosure. Howarth believes that practising and academic defamation lawyers alike should be aware of what the *Reynolds* defence has done, and is currently doing:

> 'We are shifting risks of a serious form of harm away from the media and onto potential victims, discouraging participation in public life, expecting much more of judges in setting appropriate standards and increasing costs per case. The question reformers should constantly ask themselves is whether these are prices worth paying.'[1286]

[1283] *Economou v de Frietas* [2018] EWCA Civ 2591[81].
[1284] Ibid [86].
[1285] *Loutchansky v Times Newspapers* [2001] EWCA Civ 1805; [2002] QB 783; [2002] 2 WLR 640; [2002] 1 All ER 652; [2002] EMLR 241.
[1286] Howarth above, n 1227 at 877.

Indeed, in the post-2013 case of *Yeo*, the High Court observed that the *Reynolds* defence (which it deemed synonymous with the section 4 defence), is objectively *easier to prove* and run that that of the truth defence:

> 'This defence sets a lower threshold than justification. It should be less challenging to establish that the articles represented responsible journalism on a matter of public interest than to prove their substantial truth…' [1287]

Perhaps what has now happened is that an already lenient defence in defamation (*Reynolds*) has become even easier for defendants to rely on. Early signs certainly seem to suggest this – particularly with regards to the expansive decision in *Economou* above. Howarth issued his above warning in 2011 before the adoption of the new Act. However, the quotation above serves as a stark reminder of the impact upon society that an unduly liberal interpretation of the new defence could generate.

vi. The interaction between the defences of 'honest opinion' and 'publication on a matter of public interest'

A new aspect of the 2013 Act that has caused controversy is the second overlap between the section 3 defence of honest opinion and the public interest defence within section 4. Section 4(5) states:

> '(5)For the avoidance of doubt, the defence under this section may be relied upon irrespective of whether the statement complained of is a statement of fact or a *statement of opinion*'.[1288]

This extends the application of the public interest defence to cover statements of opinion that are in the public interest, as opposed to publications that solely focus upon facts – so section 4 therefore covers facts as well as opinions. This is a yet another overlap between the section 3 and section 4 defences.[1289] It is also another means of broadening the scope of the section 4 defence: statements of opinion could fall to be protected under section 4, and a defendant

[1287] *Yeo MP v Times Newspapers* [2014] EWHC 2853 (QB) [128].
[1288] Defamation Act 2013 [emphasis added].
[1289] The section 3(4)(b) and section 4 crossover (in that statement protected by section 4 that are not true can be relied on as a supporting 'fact') has been discussed earlier in this chapter.

could pursue this avenue if their opinion failed to be protected under the section 3 defence (and its several requirements) but could satisfy section 4's requirements of public interest and reasonable belief. It is submitted here that this additional overlap between the two defences is confusing and merely serves to extend the number of scenarios that the public interest defence applies to, once again prioritising expression over personality rights.

III. Section 5 of the Defamation Act 2013: The liability of a website operator for defamatory content posted by a third party

The next section of this chapter will discuss a new addition to defamation law in England and Wales; the specific provisions in the new Act concerning website operator liability for hosting defamatory content posted by third parties to their site. In essence, it shields website operators from liability in defamation when they themselves have not posted the defamatory content at issue to their website. This has increasingly become a problem in the digital generation, as many individuals are now hosting websites which are interactive platforms on which other people can comment.[1290] This new liability mechanism is found in section 5 of the Defamation Act 2013 and the Defamation (Operators of Websites) Regulations 2013.[1291] Out of the defamation-oriented data dissemination scenarios listed at the beginning of this chapter, two in particular are engaged here: scenario ii where a social media site such as Facebook hosts defamatory pieces or content posted by person Z about person Y and scenario iii, where a website which has posted an article concerning a particular issue draws comments posted by third party users which are defamatory about person Y. Section 5(1) notes the purpose of the defence: 'this section applies where an action for defamation is brought against the operator of a website in respect of a statement posted on the website.'

Section 5(2) of the 2013 Act states that:

> '(2)It is a defence for the operator to show that it was not the operator who posted the statement on the website…'

[1290] As of June 2018, there were 1,630,322,579 websites on the internet. See 'Total number of Websites' (*Livestats*, June 2018) accessible at: https://www.internetlivestats.com/total-number-of-websites/ (last accessed 28/8/19).
[1291] The Defamation (Operators of Websites) Regulations 2013, Statutory Instrument No.3028.

Section 5 continues, and notes that:

'(3)The defence is defeated if the claimant shows that…

(b)the claimant gave the operator a notice of complaint in relation to the statement, and

(c)the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.'[1292]

This means that the additional regulations come into effect[1293] if a claimant makes contact with a website operator requesting that defamatory material posted by a third party on the host's site be removed. The regulations require the website host to act rapidly, paragraph 2(1) stating that that an 'operator must, within 48 hours of receiving a notice of complaint'[1294] make the third party aware that their post has been complained of and ask them whether they consent to their comment being deleted. Once a third party 'poster' has been contacted regarding the complaint, they have several options to move forward, set out in paragraph 2(2) of the regulations:

'(2) To comply with this sub-paragraph the response must—

(a)inform the operator whether or not the poster wishes the statement to be removed from the locations on the website which were specified in the notice of complaint; and

(b)where the poster does not wish the statement to be removed from those locations—

(i)provide the poster's full name;

(ii)provide the postal address at which the poster resides or carries on business; and

(iii)inform the operator whether the poster consents to the operator providing the complainant with the details mentioned in paragraphs (i) or (ii).'

[1292] Section 5(3)(b) and (c) of the Defamation Act 2013.
[1293] The following section reflects the section 5(2) defence for operators of websites in the Defamation Act 2013 – the regulations flesh this defence out.
[1294] Within 48 hours of the notice of complaint from a claimant - The Defamation (Operators of Websites) Regulations 2013, Statutory Instrument No. 3028, Regulation 3, Paragraph 2(1). See: https://www.legislation.gov.uk/ukdsi/2013/9780111104620 (last accessed 19/4/18).

If the third party doesn't consent to the information's removal under section 2(a) above then they must provide their real name and contact details as required under section 2(b); these will be passed on to the claimant who can pursue a defamation action against the third party separately.[1295] The regulations also account for a lack of response from a third party poster. They detail that:

> '(1) This paragraph applies where the operator acts in accordance with paragraph 2 in respect of a notice of complaint and the poster fails to respond within the period specified in paragraph 2(1)(b)(i) [5 days].
>
> (2) Where this paragraph applies the operator must, within 48 hours of the end of that period—
>
> (a)*remove the statement from the locations on the website* which were specified in the notice of complaint; and
>
> (b)send the complainant notice in writing that the statement has been removed from those locations on the website.'[1296]

The result of the above is that if an operator *cannot* contact the third party poster or the individual doesn't respond within five days, the operator must remove the statement complained of.[1297] Provided website operators comply with these rules, they cannot be sued for defamation with regards to the statement, as per section 5(2) of the Act (above).

Section 5's inclusion must be commended in the sense that it has attempted to address the problem of online defamation and acknowledged that this is, in the digital world, an increasingly prevalent issue. It must be noted that these regulations serve to act as a 'shield' to protect website operators from legal action and also a 'sword' to data subjects, in the sense that content can be removed or a third party poster sued. On initial assessment, the regulations appear to provide some sort of balance between the rights of a data subject to take action against a wrongful party and the rights of a website operator in protecting their business from a flood of legal claims. These are the same set of values which hang in the balance as per the example of data dissemination scenario iii discussed at the outset of this

[1295] Ibid, Regulation 3, Paragraph 2.
[1296] Ibid, Regulation 3, Paragraph 5 [emphasis added].
[1297] Ibid, Regulation 3, Paragraphs 2, 5 and 7.

chapter (*where a website publishes an article which attracts defamatory comments*). Although the regulations do provide some route to redress for a claimant (for example, in the scenario where the third party poster does not acquiesce to their comment being taken down, their details can be passed on) there are some aspects of the rules that may disadvantage a data subject.

For example, according to the regulations the default approach is that, if in doubt, potentially defamatory comment will be left visible on the host's site; in other words, the default position of a host website should be to disclose. This is the case as section 2(2) (extrapolated above) is complied with by a website host handing over the contact details of a third party poster if such a poster 'does not wish the statement to be removed'.[1298]A comment will remain accessible while the host contacts the third party poster[1299] and a comment will remain online in the eventuality that the third party has been contacted, but wishes to pass their details on rather than agree to the comment being taken down.[1300] The argument central to this thesis is that there is an imbalance online with regards to the amount of personal information freely accessible and few methods of retracting it. This default approach of section 5 in endorsing disclosure in the interim before further action is taken reinstates an imbalance rather than rectifies it.[1301]

A question that also remains unanswered is whether these regulations apply to social media sites such as Facebook where an individual poster can be contacted directly by a claimant in the event that they are not anonymous.[1302] A plausible interpretation of the 2013 regulations

[1298] The Defamation (Operators of Websites) Regulations 2013, Statutory Instrument No. 3028, Regulation 3, Paragraph 2(2)(b). See: https://www.legislation.gov.uk/ukdsi/2013/9780111104620 (last accessed 19/4/18).
[1299] Ibid, Regulation 3, Paragraph 2(1).
[1300] Ibid, Regulation 3, Paragraphs 2(2) and 8.
[1301] This is not unusual in the context of defamation. However, applying this rule in the context of defamatory content online can be argued to be flawed – due to the imbalance between free speech and personality rights online, firmly in speech's favour. There is an argument to be had that it would have been better in this context to suggest that the content could, under section 5, be taken down pending an action in defamation. This would have made the section 5 regulations more in line with procedure undertaken when copyright infringement has been 'flagged' on YouTube videos: YouTube's policy is to initially take down a video that has been flagged or 'striked', further action can then be taken by the 'striker' against the video's owner. This can also be appealed or no further legal action taken on the part of the striker, which could lead to the video being reinstated. See: 'Copyright strike basics' (*YouTube Help*, 2019) accessible at: https://support.google.com/youtube/answer/2814000?hl=en-GB&ref_topic=9282678 (last accessed 28/8/19). Also see commentary channel Zachary Michael on YouTube who discusses his experience in this regard: https://www.youtube.com/watch?v=S9LKu2n7NkA&list=PL2xCUcXi8awoJqtNSBb1JhBTyDXhcVs10&index=5&t=0s (last accessed 28/8/19).
[1302] There has also been the rise of anonymous social media sites: see Denzil Correa, Leandro Araùjo Silva, Manaick Mondal, Fabrício Benevenuto, Krishna P. Gummadi, 'The Many Shades of Anonymity: Characterizing

would be that they do not, as they protect a website operator from liability in the event that a poster can be contacted by the claimant (the operator having facilitated this) and action taken against them.[1303] If section 5 is interpreted in this manner, concerns can be raised with regards to how identifiable an individual poster is on a given social media website. Many individuals choose to use pseudonyms on social media[1304] and some profiles may have specific privacy settings where an individual cannot be contacted. This casts doubt over the ability of a claimant to find out key information[1305] about a person whom they wish to take an action against. It is submitted that for these reasons, the English courts must seek to apply section 5 to social media websites, as to equip data subjects with the information needed to sue a third party poster. If a large and powerful website host such as Facebook were to directly message a seemingly anonymous user, they may be more likely to receive a response as opposed to a claimant (often a private individual, with less influence). If there was no response to the host, a data subject would receive redress in the form of deletion, in accordance with the regulations set out earlier.

i. *Delfi AS v Estonia*

The set of controversial judgments at Strasbourg of *Delfi AS v Estonia* dealt with specific issues surrounding intermediary liability.[1306] The facts of this case strongly align with data dissemination scenario iii as discussed at the introduction of this chapter – a scenario where a website posts an article online which attracts a slew of defamatory comments. This case provides an interesting point of comparison with section 5 of the Defamation Act and its regulations, as it was high-profile (it went to the Grand Chamber at the ECtHR) and it

Anonymous Social Media Content (2015) Association for the Advancement of Artificial Intelligence, accessible at: https://socialnetworks.mpi-sws.org/papers/anonymity_shades.pdf (last accessed 10/9/18).

[1303] When the website host passes the personal details of the third party poster on according to 8 (2) (b) The Defamation (Operators of Websites) Regulations 2013, Statutory Instrument No. 3028, Regulation 3, Paragraph 8(2)(b) See: https://www.legislation.gov.uk/ukdsi/2013/9780111104620 (last accessed 19/4/18).

[1304] In fact, many sources encourage the user of pseudonyms online for data protection reasons. This is particularly common among individuals who like to 'troll' on the web (antagonise others through controversial posts). A common threat on internet forums is being 'doxxed': personal information about you, such as your name and address, released. See Steven Mazie, 'Why you need to get yourself a pseudonym' (*Big Think*, 28 August 2014) accessible at: http://bigthink.com/praxis/why-you-need-to-get-yourself-a-pseudonym (last accessed on 19/4/18).

[1305] In other words, their name and address. Many social media users do not advertise their addresses on their personal profiles, so this particular information would be particularly difficult for a claimant to obtain on their own without the consent of the third party poster.

[1306] *Delfi AS v Estonia* App no 64569/09 (ECHR, 10 October 2013) and *Delfi AS v Estonia* App no 64569/09 (16 June 2015), hereafter '*Delfi 2013*' and '*Delfi 2015*' respectively.

concerns the responsibility of website hosts for unlawful content posted to their sites by third party users. It may influence the English and Welsh courts with regards to how they approach section 5's regulations[1307] and give some indication on how English judges will adjudicate on section 5 in the future.

The judgments concerned Delfi, an online news website. The site publishes hundreds of articles a day and is one of Estonia's large news portals, operating across several other Eastern European states.[1308] It implemented a comment policy on its website similar to that of the abovementioned UK news site, *Mail Online.*[1309] Individuals had the opportunity to click a button to add their own comments attached to a news article which could be read by the public at large. The commenter's name would appear below the comment as well as an email address (the provision of which was not essential), however, the majority of comments were posted under pseudonyms.[1310] Comments were uploaded by default and were not generally moderated by Delfi.[1311] A notify-and-takedown policy was operated for 'hate' comments and there was an automatic deletion mechanism or filter for comments containing obscene words.[1312] The case centred upon an article which concerned a shipping company which was said to have 'destroyed a planned ice road' between frozen islands and mainland Estonia.[1313] Person 'L' was a majority shareholder of the shipping company at this time, and twenty of the comments on the article personally attacked L, using threats and offensive language.[1314] L's lawyers requested that Delfi removed the comments and give compensation for non-pecuniary damage; Delfi removed the offensive comments but refused to pay any damages.[1315] In domestic proceedings, in June 2008 the domestic Harju County Court found in favour of L, noting that Delfi's notice-and-takedown policy was 'insufficient and did not allow adequate protection for the personality rights of others.'[1316] In addition, it found that the website was a 'publisher of the comments',[1317] and that freedom of expression did not cover

[1307] Due to interpretive obligations imposed on the courts under the Human Rights Act – such as that in section 3(1): 'So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights.'
[1308] *Delfi 2013* [7].
[1309] *Mail Online*, the website of the UK newspaper The Daily Mail, accessible at: http://www.dailymail.co.uk/home/index.html (last accessed 19/4/18).
[1310] As is the case with the vast majority of news website portals.
[1311] *Delfi 2013* [8].
[1312] Ibid [9].
[1313] Ibid [12].
[1314] Ibid [13].
[1315] Ibid [14].
[1316] *Delfi 2015* [26].
[1317] Ibid.

the comments made to the detriment of L's reputation.[1318]The County Court awarded L with 320 Euros in damages.[1319] The Tallinn Court of Appeal upheld this decision, and the Supreme Court later dismissed a further appeal by Delfi, adding that they agreed with the Court of Appeal's finding that Delfi was not prohibited from being liable according to the Estonian 'Information Society Services Act'.[1320] The ECtHR also noted that Article 17 of the Constitution of the Republic of Estonia states that 'no one's honour or good name shall be defamed' and Article 45 noted that 'everyone has the right to freely disseminate ideas, opinions, beliefs and other information by word, print picture or other means…'[1321] The Estonian Information Society Services Act contained regulations pertinent to the case, namely:

> 'Section 8 – Restricted liability in the case of mere transmission of information and provision of access to a public data communications network
>
> (1) Where a service is provided that consists of the mere transmission in a public data communication network of information provided by a recipient of the service, or the provision of access to a public data communication network, the service provider shall not be liable for the information transmitted, on condition that the provider:
>
> 1. does not initiate the transmission;
> 2. does not select the receiver of the transmission; and
> 3. does not select or modify the information contained in the transmission.
>
> (2) The acts of transmission and of provision of access within the meaning of subsection 1 of this section include the automatic, intermediate and transient storage of the information transmitted, in so far as this takes place for the sole purpose of carrying out the transmission in the public data communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.'[1322]
>
> 'Section 10 – Restricted liability in the case of provision of an information storage service

[1318] Ibid [27].
[1319] Ibid.
[1320] Ibid [28-31].
[1321] Ibid [33].
[1322] Ibid [39].

> "(1) Where a service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that:
>
> 1. the provider does not have actual knowledge of the contents of the information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;
>
> 2. the provider, upon obtaining knowledge or awareness of the facts specified in indent 1 of this subsection, acts expeditiously to remove or to disable access to the information.
>
> (2) Subsection 1 of this section shall not apply when the recipient of the service is acting under the authority or the control of the provider.'[1323]

Delfi complained that its Article 10 rights had been infringed by the domestic courts' decisions that it was liable for the comments on its news portal by third parties.[1324]

a. The First Section judgment

In a controversial decision, the first section judgment concluded that although the article that Delfi published was not itself defamatory, the company should have had the foresight to know that it was on a particularly contentious issue and that it ought to moderate the page because a large amount of (negative) comments would be generated by it.[1325] The Court also found that the 'word based filter' that Delfi had installed was ineffective in blocking defamatory content,[1326] and that the website's notice-and-takedown policy did not guarantee sufficient protection for the personality rights of others.[1327] As a result of these three findings, the Court held that there had been no violation of Article 10 ECHR.

In reaching its conclusion, the Court balanced the competing rights of Delfi as an online host and L's personality rights.[1328] In adjudicating this balancing exercise, the Strasbourg Court relied upon a modified version of balancing factors that it considers when deciding upon privacy claims when Articles 8 and 10 ECHR compete. It transformed the privacy–related

[1323] Ibid [39].
[1324] Ibid [59].
[1325] *Delfi 2013* [86].
[1326] Ibid [87].
[1327] Ibid [89].
[1328] Ibid [92].

factors of i) general interest, ii) fame of claimant, iii) subject of report, iv) prior conduct, v) method of obtaining information and vi) consequences of the information[1329]into a new list relating to third party comments online.[1330] This new list comprised of:

1. Context of the comments;
2. Measures applied by the intermediary company to prevent or remove comments;
3. The possible liability of the third party authors of the comments as an alternative to the company's liability;
4. The consequences of the domestic proceedings for the company.[1331]

The Court held that Delfi had at least constructive knowledge to the effect that the article they had posted was contentious and likely to receive negative comments, and therefore it should have been more vigilant in moderating them.[1332] The Strasbourg Court also noted the relevance of the lack of a mandatory requirement on the part of Delfi of a user to register prior to commenting on articles.[1333] This was a problem as it meant that Delfi (as an intermediary) may not be able to contact a third party poster to discuss the removal of a comment. The Court stressed that a website operator would have more resources at its disposal to monitor the content on its website and appeared to suggest that the obligation should be shifted to a website to delete defamatory information, rather than for a claimant to report it.[1334] Therefore, as stated above, the Court found no violation of Article 10.

i. The parties' arguments and their interaction with English defamation law

Delfi argued in the case that the Estonian national court in holding it liable for the third party's comments contravened Article 10.[1335] In its defence, the Estonian government argued that:

[1329] This is a list of factors used extensively in Strasbourg (and to an extent, English) caselaw which is employed when balancing Articles 8 and 10 in invasion of privacy cases. See *Von Hannover (No.2)* and *Weller v Associated Newspapers Ltd* High Court (Queen's Bench Division) [2014] EWHC 1163 (QB), [2014] E.M.L.R. 24.
[1330] *Delfi 2013* [83].
[1331] Ibid [86].
[1332] Ibid [86].
[1333] Ibid [90].
[1334] Ibid [92].
[1335] Ibid [46].

> '…placing the obligation to monitor the comments and notify the portal administrator of offensive comments on the possibly *injured parties* was *neither sufficient nor justified*. Such a system did not ensure sufficient protection of the rights of third parties, as proven by the circumstances of the present case.'[1336]

The Estonian government appeared to be implying that placing an obligation upon a data subject to notify a website of defamatory content is inefficient; it takes time for a data subject to find or become aware of such content about themselves, and it takes time for a host website to take action upon notice. The Estonian government also linked this inefficiency back to a likelihood of increased damage to personal dignity and personality rights. Additionally, the government seemed to take the view that to place the obligation upon a data subject was morally wrong, through the use of the phrase 'nor justified'. This is a position that this thesis endorses – it appears in the very least unfair to place yet more responsibility on an individual data subject to protect their own personality rights, rather than companies which seek to make profit over the disclosure of personal information.[1337]

The government also noted that:

> 'Any information communicated via the Internet spread so quickly that by the time the inappropriate comments were finally deleted the public interest in the given news and the comments posted on it had waned. Measures taken weeks or even days later for protecting a person's honour were no longer sufficient, because offensive or unlawful comments had already reached the public and *done their damage*…'[1338]

b. Grand Chamber decision

The First Section judgment was appealed and the matter was heard by the Grand Chamber. The Chamber concurred with the First Section's judgment and held that Article 10 had not

[1336] Ibid [63].
[1337] As a point of interest, the Estonian government also noted that Delfi was a 'profit oriented' company which had an interest in third parties posting comments upon their news pieces. See *Delfi 2013* [64].
[1338] Ibid [63].

been violated by the decision of the Estonian courts.[1339] The court powerfully observed that a news website should be aware of the impact of their activity and the content displayed on their website, Woods noting that 'the idea that a news portal is under an obligation to be aware of its content is a key element' of the judgment.[1340] The Court also observed that audio-visual media 'often have a much more immediate and powerful effect than the print media.'[1341] Indeed, the Court went on to state that it was relevant that an internet portal operator is a publisher or a discloser for financial gain.[1342]

A further interesting aspect of the Grand Chamber's judgment is that it distinguishes news portals from websites that do not generate their own content, the example being given of social media sites.[1343] The implication of this distinction appears to be that a social media site would not be held accountable as an intermediary in the same way that a news portal would, partly because it is a mere conduit for personal data and does not create its own material and is therefore not a 'publisher'.[1344] It is submitted that this distinction is not as straightforward as the Strasbourg Court seems to believe – in modern times, many social media sites have started using a mixture of user-generated content and their own content (perhaps outsourced from third parties) to remain relevant and for financial gain. Facebook has resorted to embedding linked articles to other websites within homepages as well as inserting copious advertisements into its users' 'newsfeed'; the platform in 2019 looking markedly different to when the website first became accessible to the public.[1345] It also hosts content from third parties.[1346] The landscape of social media is now different to that which existed only several years ago – even successful sites have sought to broaden the type of content they host in order to remain contemporary and economically viable. If the Strasbourg Court is to continue

[1339] *Delfi 2015* [162].
[1340] Lorna Woods, 'The Delfi AS v Estonia judgment explained' (*LSE Media Policy Project Blog*, 16 June 2015) accessible at: https://blogs.lse.ac.uk/mediapolicyproject/2015/06/16/the-delfi-as-vs-estonia-judgement-explained/ (last accessed 2/9/19).
[1341] *Delfi 2015* [134].
[1342] Ibid [144].
[1343] Ibid [112].
[1344] Ibid [112 and 116].
[1345] Facebook, 'Branded Content, 'Overview' accessible at: https://www.facebook.com/facebookmedia/get-started/branded-content (last accessed 23/4/18).
[1346] See Mike Murphy, 'Snapchat is becoming the anti-Facebook' (*Quartz*, 29 November 2017) accessible at: https://qz.com/1141464/snap-is-redesigning-snapchat-to-split-up-messages-from-friends-and-brands-snap/ (last accessed 23/4/18) and Emily Tan, 'Samsung is first brand in UK to try out Snapchat's new sponsored animated filters' (*Campaign*, 22 December 2017) accessible at: https://www.campaignlive.co.uk/article/samsung-first-brand-uk-try-snapchats-new-sponsored-animated-filters/1453368 (last accessed 23/4/18).

to differentiate between news portals and social media sites in the future, it must seek to rely upon a more thorough distinction, as it appears that this one has been eroded.[1347]

The final point to note regarding the judgment in *Delfi* is that the posts in question contained hate speech and therefore the unlawful nature of the comments were, or should have been, apparent to the website host.[1348] In this respect, the judgment must be distinguished from defamation jurisprudence and legislation: if a claimant contacts a host site demanding action is taken against a 'defamatory' post, the website has no way of knowing whether the statement would be held to be defamatory content in court – the information may or may not be true, and there may be no easy way a host could find out. On the contrary, hate speech (and the parameters of it)[1349] are more obvious in comparison so a host website could reasonably be expected to act with more assurance in deleting posts of this nature. This factor in the case accounts in part for the decision of no violation, and also for the hard-line approach that the Court took against Delfi regarding their lack of action.

c. Joint dissenting opinion of judges Sajó and Tsotsoria

Despite *Delfi*'s Grand Chamber judgment being welcomed keenly by Judge Zupancic in his concurring opinion,[1350] the decision was met with opposition from Judges Sajó and Tsotsoria. In a joint dissenting opinion, both argued that the judgment imposed a test of constructive knowledge of potential defamation upon website hosts and, as a result, all comments on such sites will have to be monitored, amounting to censorship.[1351] However, what both judges fail to address is that no censorship of the news media or host-website–generated content was at issue within the case; rather, it was generic insults against L from third parties that had been requested for deletion. Indeed, academic criticism of the judgment also seems to miss – or gloss over – this point, Woods stating of the Grand Chamber and its decision:

> '…it seems to give little regard neither to its own case law about political speech, nor its repeated emphasis on the importance of the media in society.'[1352]

[1347] And was eroded at the time of the 2015 judgment. This is perhaps an example of the difficulties the judiciary have with keeping up with the ever–changing digital landscape.
[1348] *Delfi 2015* [159].
[1349] For example in English law, Public Order Act 1986 c.64 contains a clear definition of what constitutes hate speech on the grounds of race, religion and sexual orientation.
[1350] *Delfi 2015* pg. 65.
[1351] *Delfi 2015* pg. 68 onwards.
[1352] See Woods above n 1340.

This is despite the fact that no legitimate forms of news media were restricted by the ruling – just hateful and defamatory comments *annexed* to a news article. The joint dissent also does not undertake a robust assessment of the value of the expression which was curtailed as a result of the ruling – important information about the ice-road in Estonia was left visible in the article on Delfi's site, however low-value abuse in the comments aimed personally at L was removed. Taking into account this thesis' evaluation of the importance of different types of speech,[1353] an important political discussion of genuine public interest was not removed or censored by the ruling. It is also argued here that implementing a test of constructive knowledge upon website hosts regarding third party commentary is not as draconian as some may fear. News websites and other types of portals online make a conscious decision to allow or prohibit third party commentary on their websites. If an article is posted by a news portal that is particularly contentious, it is a simple exercise for a news portal to disable commentary if they do not wish to moderate the comments upon the article, or others like it. We should also recognise that these sites encourage comments in order to draw traffic to their site, for commercial gain.[1354]

It is respectfully submitted that this dissent misses the mark with regard to the competing rights at issue in *Delfi*. Because of the vast amount of personal information that is currently online and the relative ease of dissemination, it is important that protective measures are taken to ensure that there is a route to redress for those who have been defamed online, including those who have been defamed anonymously by a commentator on a news portal. If host websites are not held responsible in some way to help a claimant find redress then it would be difficult if not impossible for a data subject to enforce their personality rights online in such a circumstance.

It is argued here that the judgment in *Delfi* is not as controversial as some have claimed.[1355] The robust stance of both the First Section decision and the Grand Chamber is reflective of several key aspects of the case and its wider context: firstly, the speech in question was hate speech; secondly, the speech was low-level expression (by its nature – insults and crude

---

[1353] Chapter 4.
[1354] *Delfi 2015*.
[1355] See Woods above n 1340 and Neville Cox, 'Delfi AS v Estonia: The Liability of Secondary Internet Publishers for Violation of Reputational Rights under the European Convention on Human Rights' (2014) 77(4) *Modern Law Review* 619.

language) which had no genuine public interest value and thirdly, a general view was put forward by the Strasbourg courts that not enough was being done by website hosts to protect the personality rights of others online. In respect of the latter point, the court's view aligns with the central argument of this thesis.

d. Applying the First Section and Grand Chamber's judgments in *Delfi* to section 5, Defamation Act 2013 and its regulations

Some points of interest can be extrapolated from the First Section's and Grand Chamber's decisions in *Delfi* and be cross-applied to section 5 and its regulations. Firstly, the argument of the Estonian government with respect to the First Section's decision that 'measures taken weeks or even days later for protecting a person's honour were no longer sufficient, because offensive or unlawful comments had already reached the public and *done their damage*'[1356] can be directly applied to section 5's regulations and in particular to its system of notice and takedown that spans over five days (with an additional 48 hours after the five-day period for a host to act).[1357] This does not include the potentially significant amount of time which it has taken a data subject to become aware of defamatory content and to contact a host website. In a circumstance where a third party refuses to agree to their comment being removed from the site, it would remain accessible for months or even years while a defamation claim was filed and adjudicated upon.[1358] If a defamatory piece goes viral it can take merely hours for a large amount of people across the globe to become aware of it – in addition, the friends, family and colleagues of a data subject may have been made aware of such a comment and viewed it before it is removed under section 5's scheme. However, despite these legitimate concerns about waiting period, it must be remembered that it is for *practicable* reasons that the drafters of the Defamation Act 2013 have implemented a five-day mechanism into section 5; the third party in question may only check their emails or social media accounts over periods of several days. Placed in a wider context about defamation law, this aspect of section 5 can be viewed as compatible as ordinarily no interim injunctions are granted in respect of defamation claims and therefore defamatory materials always stays in place (sometimes for

[1356] See above.
[1357] The Defamation (Operators of Websites) Regulations 2013, Statutory Instrument No. 3028, Regulation 3, Paragraph 2. See: https://www.legislation.gov.uk/ukdsi/2013/9780111104620 (last accessed 19/4/18).
[1358] See National Audit Office, 'Efficiency in the criminal justice system' Ministry of Justice, HC 852 Session 2015-16 (1 March 2016) accessible at: https://www.nao.org.uk/wp-content/uploads/2016/03/Efficiency-in-the-criminal-justice-system.pdf (last accessed 9/5/19).

years) until a case is heard.

In the Grand Chamber, Delfi argued that the 'actual authors' of the comments should remain responsible for their contents rather than themselves, acting as a news portal.[1359] Under the section 5 of the new Act, it could be said that third party-commenters remain liable for their defamatory statements – if website operators comply with the regulations set out above,[1360] liability shifts to the third party. Section 5 strikes a middle ground between liability apportioned to the person that *made the comment* and the website *which has facilitated that comment in being made public* (a website chooses to leave comments 'on'). Section 5 is also focused on practicable remedies for the person who has been defamed – a website operator is best placed to put a claimant in touch with a defendant commentator, having access to their personal details if a commentator has signed up to the website. Larsson has observed that in the years since Delfi was decided many websites have in fact modernised the way they regulate comments, with an emphasis on user-liability – which has less to do with the ruling, he argues, and more to do with developing technology and the increased traffic to websites. He observes:

> 'News portals have since developed their instruments for reducing anonymity and increasing users' sense of accountability when posting comments. Many sites are moderating comments these days; either by demanding the commentators to log in, for example through Facebook account, or by the flipped method that no comment is published unless it is approved…'[1361]

This is yet more evidence to support that the judgment in *Delfi* was in fact less of a threat to online expression than some commentators feared. Delfi at the Grand Chamber also argued that:

> 'The applicant company also emphasised the importance of anonymity for free speech on the Internet; this encouraged the full involvement of all, including marginalised groups, political dissidents and whistle-blowers, and allowed individuals to be safe

[1359] *Delfi 2015* [77].
[1360] By either deleting the comment after a designated time period or passing the third party's details on.
[1361] Stefan Larsson, 'Images of the digital: On the European Court of Human Rights' judgment in the case of Delfi as v. Estonia' (2015) *Jurista Vards* (English translation) accessible at: https://portal.research.lu.se/ws/files/6062769/7855442.pdf (last accessed 2/9/19) 1.

from reprisals.'[1362]

Despite Delfi's claim that the case raises a free speech issue, on the facts of Delfi it is clear that legitimate freedom of expression was not curtailed by the ruling; the case concerned remarks which were clearly defamatory and hate speech against person L. Defamatory speech is unlawful, as it is false facts as published which damage someone's reputation. In terms of the 2013 Act, there is a section 4 defence (discussed earlier in this chapter) which protects the publication, online or offline, of speech in the public interest, even if it turns out to be false – so the judgments in *Delfi* and section 5's and its regulations will do little to curtail legitimate speech in the public interest.

The Estonian government argued at the Grand Chamber that Delfi as a news portal did not have to change its company policy as a result of the ruling at domestic level (for example by monitoring comments or disabling comments altogether) and the Grand Chamber concurred, finding the same – this contributed to the Chamber's holding that there had been no violation of Article 10.[1363] Similarly, it is unlikely that website operators in England and Wales will have to substantially alter their day-to-day procedures in order to be protected under section 5. This is because section 5 only comes into operation in the wake of a *notification* by a claimant, so operators will not have to turn comments off as a blanket measure. The economic motivations of Delfi in leaving comments on was repeatedly mentioned in the Grand Chamber's judgment and was a consideration in the Chamber's finding of no violation.[1364] Indeed, this could also be seen as a justification for some (limited) obligations as imposed on website operators in order to rely on the protection offered in section 5 of the Defamation Act: often website operators create and upkeep a site for commercial gain, often through advertising revenue. The Grand Chamber also noted in its decision that commenter-anonymity was a problem for claimants seeking redress for third party comments posted to websites.[1365] As discussed above, this issue has largely been addressed with regards to online defamation and section 5 – if an operator cannot get in contact with the third party, or they do not respond within a specified time-frame, then the comment is deleted, resolving the matter.

[1362] *Delfi 2015* [79].
[1363] *Delfi 2015* [83] and [161]. Also see Woods above n 1340.
[1364] Ibid [144].
[1365] Ibid [148-151].

A final point to note is that the Grand Chamber itself made certain comments in its judgment pertaining to defamation in the digital era. The Court noted that, irrespective of the balancing exercise between Articles 8 and 10, in the digital age there are new threats to personality rights online:

> 'Thus, while the Court acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights.'[1366]

Further to this, there was show of support from Grand Chamber of additional regulations for online defamation:

> 'In this particular context the Court takes into account the fact that some countries have recognised that the importance and the complexity of the subject matter, involving the need to ensure proper balancing of different interests and fundamental rights, call for the *enactment of specific regulations*…'[1367]

It appears, then, that the ECtHR is unlikely to find that there has been a violation of expression rights if an applicant applied to Strasbourg stating that obligations imposed on them by section 5 were contrary to Article 10 ECHR.[1368]

A final note on the position of internet intermediaries

A concluding point should be made here regarding the protected position of internet intermediaries in the context of other laws. According to the Electronic Commerce (EC

[1366] Ibid [110].
[1367] Ibid [128 – emphasis added].
[1368] This should be of no surprise given that the Defamation Act 2013 was drafted with a 'pro-Article 10' bias – see discussion earlier in this chapter regarding the libel reform campaign which instigated the new Act.

Directive) Regulations 2002 No. 2013, network service providers are shielded from liability (criminal or civil) for transmission of data under Article 17 the regulations, providing they meet certain requirements, such as those in Article 17 (a) to (c) which state that the service provider did not initiate the transmission of the data, did not select the recipient nor modify the information. A similar exemption applies to caching in Article 18 of the Regulations. Finally, the 2002 Regulations also shield a *service provider* from liability for hosting information, providing that the provider does not have actual knowledge of unlawful material as hosted on their site, and in the event they have become aware of it, have made a rapid attempt to remove it under Article 19(a)(i) and (ii). Furthermore, an additional layer of protection is provided to intermediaries through section 10 of the Defamation Act 2013, which states that a court does not have jurisdiction in defamation with respect to individuals who are not the *author*, *editor* or *publisher* of the statement unless it is not practicable to bring such an action against an author, editor or publisher; the definitions of each the same as those in section 1 of the Defamation Act 1996.

To conclude, in this chapter's comparison of *Delfi*'s two judgments to section 5 of the Defamation Act 2013, an attempt has been made here to show that an effort on the part of the legislature has been made to give data subjects a remedy for when defamatory content concerning them appears online, which has sought to be practicable and balance competing interests of claimants and website hosts.

IV. Critique of section 8 of the Defamation Act 2013: The single publication rule

The final addition to the 2013 Act to be discussed in this chapter is the 'single publication rule' within section 8.[1369] This is now in place of the 'multiple publication rule' that stated that every new republication of a defamatory statement gave rise to a new claim, and was thought to be unfair towards defendants, creating 'potentially perpetual liability'.[1370] The 'old' multiple publication rule that section 8 replaces came from the case of the *Duke of Brunswick v Harmer* in 1950 – the case holding that the sale of a seventeen year old newspaper which contained a defamatory statement meant that publication had happened

[1369] Defamation Act 2013.
[1370] *Mullis Windmill*, 102.

anew, and an action in defamation proceeded.[1371] The thrust behind this rule was that with every 'new' publication, fresh reputational harm could arise – as material continued to be circulated. Mullis and Scott note that the old rule had been long criticised by expression advocates who claimed that the rule was out of touch and 'antediluvian'.[1372] In particular, concerns were raised that the law as it stood would discourage the operation of internet archives – leaving operators vulnerable to repeated actions in defamation.[1373] Section 8 has altered this *Duke of Brunswick* rule – it states that there is now a limitation period of one year (time starting to run after the first publication has been issued), after which it bars any action taken against the republication of the defamatory publication *in substantially the same form*.[1374] As such, Article 8 of the Defamation Act 2013 could engage data dissemination scenario iv as highlighted at this chapter's introduction: *where person Z retweets a defamatory piece about person Y*. Article 8's alteration of the *Duke of Brunswick* rule is of relevance to this thesis as it represents further erosion of the protection of personality rights under the 2013 Act – the Act choosing to change the rule which previously protected the Article 8 rights of individuals in order to *encourage* expression online. The first issue to consider under this new rule is what constitutes a publication in 'substantially the same' form. Section 8 gives some guidelines, stating:

> '4) This section does not apply in relation to the subsequent publication if the manner of that publication is materially different from the manner of the first publication.
>
> (5) In determining whether the manner of a subsequent publication is materially different from the manner of the first publication, the matters to which the court may have regard include (amongst other matters)—
>
> (a) the level of *prominence* that a statement is given;
>
> (b) the *extent* of the subsequent publication.'[1375]

'Level of prominence' may relate to the degree of focus which is placed on any allegation within a piece (for example, is the claimant subject of a headline?) and how easy an allegation is to find – an example given by the Act's Explanatory Notes is if the allegation is

[1371] *Duke of Brunswick v Harmer* (1950) 175 ER 441.
[1372] *Mullis Windmill*, 102.
[1373] Ibid.
[1374] Defamation Act 2013, Section 8(1)(b).
[1375] Defamation Act 2013 [emphasis added].

on a webpage, how many 'clicks' of a mouse it would take for a reader to access it.[1376] Perhaps the degree to which it is discussed throughout a publication and the level of detail could also be relevant considerations with regards to 'prominence'. This is closely related to the notion of 'tone' of a piece, a factor that has historically had significance to the *Reynolds* defence in the English courts. In *Cumpana v Romania*, an article's 'virulent' language was deemed relevant to whether the Article 10 rights of the defendant defamer were infringed.[1377] Furthermore, in *Pfeifer v Austria* the court noted that the fact that the defamatory piece was written in an aggressive and hostile style contributed to the finding that the Article 8 rights of the claimant had been infringed.[1378] In relation to section 8, the focus would not be upon whether the tone of the piece contributed to a finding that a remark was defamatory, rather whether the tone in both publications was the same – and therefore the level of prominence given to allegations in both articles the same.

The 'extent' of the subsequent publication appears to relate to how widely the defamatory content was circulated. It may be the case that a court interprets this section as suggesting that if a similar circulation was present with regards to both publications they are more likely to be viewed as substantially the same. An alternative reading would be that if the subsequent publication's circulation was more modest than the former they are increasingly likely to be viewed as in substantially the same form as little additional reputational harm will be done by the second publication if only few have seen it – this would be a practicable rather than a literal reading of the section. The converse could also apply. In interpreting this section, a court would likely closely scrutinise the degree of readership of the second publication.[1379]

For the purposes of this thesis, whether the publication of a paper-print article *online* (at a later date) would be considered in 'substantially the same' form is a pivotal question. Indeed, the degree of effect section 8 will have upon data subjects hinges upon whether online content will be deemed the same as its version in print. If it is not, then this second

[1376] Defamation Act 2013 Explanatory Notes, Section 8, paragraph 63. Accessible at: http://www.legislation.gov.uk/ukpga/2013/26/notes/division/5/8 (last accessed 13/9/18). Also see David Hooper, Brid Jordan, Kim Waite and Oliver Murphy, 'The New Defamation Act 2013: What difference will it really make?' (*Media Law Resource Centre*) available at: http://www.medialaw.org/component/k2/item/1815-the-new-defamation-act-2013-what-difference-will-it-really-make (last accessed 13/9/18).
[1377] *Cumpănă and Mazăre v. Romania* App no 12556/03 (ECHR, 15 November 2007).
[1378] Although the courts also noted that it was not a decisive factor. *Pfeifer* above, n 1114 pg. 14 (Judge Loucaides' dissent).
[1379] Questions would arise such as: was the newspaper it was circulated in popular? Was it available in only parts of the country or the whole of the UK? Did the website generate a lot of traffic? Did the post get many 'hits', 'likes', or reposts?

publication online would be actionable, protecting reputational interests.[1380] However, initial outlook for this interpretation of section 8 is not good. The Joint Committee[1381] has suggested that putting something on the internet would *not* constitute a materially different publication,[1382] despite the fact this poses a significant risk of increased readership (and potentially a factor at issue under section 8(5)(b), as discussed above). As noted above, one of the founding principles behind the inclusion of this section in the new Act was to protect data storage through internet archives, which again would point to a reading that simply republishing something online in of itself would not be viewed as materially different.[1383]

Mullis and Scott have argued that the ultimate effect of section 8 will be to penalise those who are defamed online.[1384]With every republication, regardless of whether the content is in a different form, new readers will be garnered and more reputational harm will be done.[1385] Indeed, this is where the reputational harm stems from in data dissemination scenario iv, where a person retweets defamatory content – the mere fact that information has spread further can damage personality rights. Torts are created to respond to harm caused and section 8's new rule has the potential to hinder justice as well as Article 8 rights.[1386] Mullis and Scott have also argued that past criticism of the original multiple publication rule was 'wilfully one-eyed',[1387] the pair stating:

> 'When Lord Lester mused on the fact that whereas 'the Duke of Brunswick sent his valet to obtain a 17-year-old publication of the *Weekly Dispatch* . . . now search engines do the same thing thousands of times per day', he could see only the ramifications of the extant rules for freedom of expression. The new rule can be criticised correspondingly as wrong in concept because it *elides the harms caused by ongoing publication*. Reputational harm is caused not by the act of publication (in its everyday rather than legal sense), but rather when the reading occurs.'[1388]

[1380] See Howarth above, n 1227 at 866.
[1381] See above, n 1245.
[1382] See Gavin Phillipson above, n 1141 at 182.
[1383] See 'Defamation expert: New '1 year after publication' rule means an easy life for UK libel judges' (*The Register*, 7 January 2014) accessible at: https://www.theregister.co.uk/2014/01/07/single_publication_defamation_reform/ (last accessed 13/9/18).
[1384] *Mullis Pendulum* at 56.
[1385] Ibid.
[1386] Ibid, 57.
[1387] *Mullis Windmill* at 103.
[1388] Ibid [emphasis added].

In a quest to reaffirm Article 10 interests using the new Act, it is argued that Article 8 rights have, certainly in the case of section 8, fallen by the wayside. In a move to quieten criticisms of the multiple publication rule as punitive to defendants, the single publication rule now tips the balance in the opposite direction and is unduly restrictive towards claimants. As Mullis and Scott observe, little thought appears to have been given to the harm done by repeated publications. With every new publication of an allegation a fresh set of reputational harm can be done. New people may read republished allegations and people who had once read the past allegations may find their negativity towards a claimant rekindled afresh, that which had been previously forgotten.[1389] A new set of social bonds may be ruptured by a republication (new friends may have been made by a claimant in the interim) and a claimant's feelings of low self-worth may once again rise up and take hold, perhaps in a stronger way than before as they may have thought that they had been given a chance to move on with their lives and put past allegations behind them.

Section 8's prioritisation of Article 10 rights over Article 8 interests is clear, particularly in light of the ECtHR's current position that the right to reputation is encompassed by Article 8.[1390] Mullis and Scott as well as Phillipson argue that due to section 3 of the Human Rights Act 1998 – which places an obligation on the courts to interpret legislation compatibly with the ECHR – the courts may have to realign this balance by making use of their 'equitable' ability to lift section 8's ban under discretionary powers conferred by the Limitation Act 1980.[1391] The factors the courts could consider relevant to lift section 8's ban would include whether the claimant will be prejudiced by it, the reasons for any delay to taking action and whether a claimant was unaware of any facts giving rise to an action (if they were unaware of the defamatory comment up until a certain point).[1392]

To conclude, the Act's introduction of the section 8 rule is problematic not only due to its negative impact on data-rights and reputation but also through its lack of compatibility with the ECHR. It appears to be an ill-thought out move to prioritise expression, with little thought being given to the marginalisation viable claims. Due to potential clashes with Article 8, this

[1389] Schönberger makes a point of memory in his monograph, arguing that the ability for people to forget and move on in their lives is crucial – a republication would stop someone from doing this. See *Delete*.
[1390] See chapter 3.
[1391] Section 8(6)(a) Defamation Act 2013 and section 32A Limitation Act 1980, *Mullis Windmill* at 103 and Phillipson above, n 1141 at 183-5.
[1392] Section 32A Limitation Act 1980 sections 1(a), 2(a) and (b) respectively.

aspect of the Act is ripe for development through future caselaw. In this regard, the section's flexibility is its saving grace; it only proffers two factors towards how to interpret 'material difference' in form (the court being free to use 'other matters' to come to a decision)[1393] and incorporates the Limitation Act 1980 which gives courts the equitable scope to defer from section 8's limitation period. Perhaps this section of the new Act is the 'one to watch'.

Conclusion

This chapter has sought to consider the ability of a private individual within England and Wales to seek redress regarding defamatory content (damaging to their reputation) online circa 2019. To analyse this, an assessment of various aspects of defamation law and the new 2013 Act has been conducted. Some interim conclusions have been reached along the way. Firstly, aspects of the Act's section 3 defence of honest opinion have made it more difficult for claimants to successfully argue a defamation claim, be it online or offline – as the defence has taken an increasingly pro-defendant stance in its codification. The requirement of the defence for a defendant to adduce a supporting fact is now wholly objective, in that a defendant does not have to prove that *they were actually aware of those facts at the time* – rather, those facts merely had to exist at the time the comment was made. The removal of the defence's public interest requirement has also broadened the defence and made it increasingly easy for a defendant to rely on it. Secondly, it has been argued that there is a lack of legal certainty surrounding section 4's codification into statute (formerly the *Reynolds* defence). It is unclear whether there has been any true reform with regards to section 4 (Lord Nicholls' laundry list of factors are still relevant to *some* extent) and a wide reading of 'reasonable belief' *that a publication is within the public interest* within section 4 could hinder Article 8 rights. Extending the defence to cover citizen journalists online could also unfairly encroach on reputational interests and the removal of the requirement that a decision to publish be 'responsible' within section 4 has additionally broadened the scope of the new defence, once again prioritising Article 10 interests over personality rights. The complex overlap between the section 3 and section 4 defences has also tipped the balance in favour of defendants – as an incorrect statement protected by a section 4 defence can be used to bolster a section 3 defence in a separate action (potentially resulting in a claimant's action being defeated despite the fact an honest opinion of the defendant was based on false facts). By way of

[1393] Section 8(5) Defamation Act 2013.

positive developments, section 5 of the Act attempts to give some redress to data subjects through its regulations regarding defamatory content posted to websites by a third party, at the same time as shielding host websites from liability. Finally, section 8 represents a blow to personality rights under the 2013 Act's provisions – a bar on action has been enforced after a year has passed from a statement's initial publication if the defamatory remark is in substantially the same form. Section 8 of the Act possibly represents the most naked prioritisation of expression over reputation – little thought appears to have been given as to the harm done to a data subject that this republication could cause (*even if it is in the same form*). The result of this assessment is, then, that it may well be difficult for a data subject to seek redress for online defamation for any of the aforementioned reasons – with the exception of section 5 and its regulations. It is unfortunate that the new Act has sought to prioritise freedom of expression over reputation in its text on not one but several occasions – particularly considering the reputational damage that private content online can have on a data subject be true or false information.

Overall conclusion

Several things can be concluded from the analysis conducted within this thesis. Firstly, the privacy regime as it stood prior to 2018 in English law was inadequate in its ability to cope with the deluge of personal information present online. There remains a fundamental imbalance between the vast quantities of private data on the web and the amount of privacy laws available to the public – the internet having long been seen as a place of unbridled expression. Secondly, the areas of English law that concern the rights of reputation are misuse of private information and defamation. It can be concluded from the evaluation in this thesis that the reputation-rights afforded by both of these areas are patchwork and have their own failings. It goes beyond the scope of this conclusion to reiterate all such faults,[1394]however some salient points can be noted. Firstly, misuse of private information appears to be a tort which has the strong potential to have a positive impact on privacy rights in England and Wales – and indeed it has had a progressive impact, particularly with regards to judgments which award privacy injunctions in favour of deserving claimants.[1395] However, as rehearsed at length in chapter 5, there are several reasons MPI as a tort has been ineffective in protecting privacy rights online. Firstly, in *some* High Court judgments, there has been a worrying tendency on the part of the judiciary to unfairly prioritise weak freedom of expression arguments over privacy rights. Secondly, the doctrine of 'waiver' has been relied upon to the detriment of claimants in certain MPI cases. The doctrine loosely states that *if a claimant has disclosed some amount of personal information in the past, it may be more difficult for them to assert their right to privacy in the future*. The doctrine is problematic in that it lacks logic - it does not, for example, consider a scenario where a data subject *must* speak out and disclose personal data in order to rebut false claims about themselves. More marginal notions of 'zonal waiver' have the potential to cover a large scope of personal information, the rights to which can be waived. Thirdly, the doctrine of 'information already being in the public domain' has also evolved in certain MPI cases which again has the *potential* to unfairly disadvantage claimants. In the digital era, the doctrine of 'public domain' in MPI is increasingly complex. The doctrine has traditionally appeared to state that *if information is already in the public domain, privacy rights connected with it cannot be asserted*, yet the parameters of what the public domain actually is remain blurred – and the relatively recent case of *PJS* seems to contradict the doctrine entirely, upholding an

[1394] As this would be unduly long and be repetitive of work earlier in this PhD.
[1395] Such as, most notably, the decisions in *Campbell* and *PJS*.

injunction with respect to information which had been published in several different jurisdictions and online. The modern influence of the doctrine therefore remains unclear – this is confusing for potential claimants, defendants and the judiciary (particularly in lower courts). Finally, perhaps the most significant reason that MPI has been ineffective in protecting online privacy rights is the enforcement problems that have come alongside MPI injunctions. Such an injunction is limited by its jurisdiction and there has been the widespread problem of public 'mass dissent' in ignoring the existence of injunctions and flouting them online. Damages as a remedy in MPI awards monetary compensation – as discussed in chapter 5, many such awards have been small and this does little to rectify one's reputation in practicable terms.

Defamation law, covering the publication of false and defamatory information about a data subject, also has many faults. The final chapter of this thesis has noted how small changes in wording in the codification of the defences of *honest opinion* and *publication in the public interest* (formerly known as *fair comment* and the *Reynolds* defence)[1396] could lead to future interpretations by the English courts which subtly prioritise Article 10 interests over Article 8 rights. The early section 4 (publication in the public interest) case of *Economou* in the Court of Appeal shows a willingness of the Court to broaden the scope of the defence – in this case, to include protection for 'contributors' to articles as well as potentially citizen journalists. The introduction of the *single publication rule*[1397] in section 8 of the Defamation Act nakedly prioritises the rights of publishers over those defamed by abolishing the *Duke of Brunswick* rule, and the complex interaction between the section 3 and section 4 defences will also exacerbate the speech-privacy imbalance which already exists with regards to personal information. For example, a defendant can rely on a privileged statement including one that is protected by section 4 in order to satisfy the 'basis in fact' criteria of the section 3 defence of honest opinion – even if the facts asserted within that privileged statement are not true, so there would in reality be no genuine basis in fact. Some solace should be found in section 5 of the Defamation Act and its accompanying regulations, which attempt to balance both the rights of a claimant and website operators.

[1396] Sections 3 and 4 of the Defamation Act 2013 respectively.
[1397] Ibid Section 8.

The picture that has been painted by this thesis of personality rights in English law, then, is that not enough has been done to protect Article 8 interests, despite the significant amount of personal information currently available about many individuals on the web – be it true or false. This thesis has considered whether the new right to erasure as present within the GDPR (and the Data Protection Act 2018) offers data subjects a credible avenue to assert their personality rights online through ordering the removal of personal data. It has been found that the GDPR as realised domestically provides some potential to address the failings of the both MPI and defamation in England and Wales, given that they have failed to meet (and arguably will never meet) the challenge presented by the internet to protecting personal data. The GDPR sits alongside the both torts but as a largely regulatory regime mainly aimed at data-controllers, it is fundamentally more impactful in protecting privacy and reputation online than both MPI and defamation, partially because both laws were developed to protect privacy in an off-line era. A further point of crucial contention in the right to be forgotten's ability to restate privacy online is how an erasure request will be balanced against the freedom of expression rights of the information's controller (and potentially third party-poster), particularly in light of Article 17(3)(a)'s expression exemption and journalism exemption. In chapters 3 and 4, this thesis adduced a matrix of factors derived from English and ECtHR caselaw which can be used as balancing tools by courts and national Data Protection Authorities when considering whether an erasure request should be granted in the first instance, or upheld. It has been urged here that some of the same mistakes should not be made by the English courts when interpreting this new erasure right that have been made with regards to other personality-rights at English law and at Strasbourg. It is crucial in the digital era that informational privacy is upheld, or society will undergo a shift to the worse and the negative impacts of unrestricted disclosure will be rife.

A data subject could prevent publication (or dissemination) of personal data through an injunction under MPI and in that instance the protection of informational privacy achieved might be more effective than GDPR reliance (by utilising the Data Protection Act 2018), as the right to be forgotten is an *ex-post* provision. But otherwise the GDPR regime as realised under the new Data Protection Act provides protection for online privacy, that both torts taken in conjunction are not likely to be able to provide. It seems fair to say that the right to be forgotten partially accounts for the failings of MPI and defamation, in the face of immensely increased dissemination of personal information online. In the midst of the current

influx of personal information being uploaded to the web, the problems posed by seeking to protect personal information through MPI are not resolvable. It cannot be concluded that the GDPR and the Data Protection Act 2018 provide a perfect solution to the problem of protecting private information online, making up for all the deficiencies of the two torts identified; chiefly as personal information must be disseminated online before action can be taken (as it is unclear what degree of deterrent effect the GDPR will provide) and the potentially broad reading of the right's expression or journalism exemption. However, it has been argued that its ability to protect online privacy transcends that of the two torts, especially when, in the domestic context, the provisions are interpreted in line with Article 8 ECHR, under section 3 of the Human Rights Act.

Bibliography

Primary Sources

Cases

CJEU

Bodil Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01, [2003] I-12971

C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831

Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] (ECJ) ECLI:EU:C:2014:2428

Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] W.L.R 659

Breyer v Germany [2016] (ECJ) ECLI:EU:C:2016:779

Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994

Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] (ECJ) ECLI:EU:C:2018:388

ECtHR

Dudgeon v United Kingdom App no 7525/76 (ECHR, 22 October 1981)

X and Y v The Netherlands App no 8978/80 (ECHR, 26 March 1985)

Observer and Guardian v. the United Kingdom, App no 13585/88 (ECHR, 26 November 1991)

Niemietz v Germany App no 13710/88 (ECHR, 16 December 1992)

Halford v United Kingdom App no 20605/92 (ECHR, 25 June 1997)

Bladet Tromsø and Stensaas v. Norway App no 21980/93 (ECHR, 20 May 1999)

Campmany y Diez de Revenga and Lopez Galiacho Perona v. Spain App no 54224/00 (ECHR, 12 December 2000)

Amann v Switzerland App no 27798/95 (ECHR, 16 February 2000)

Krone Verlag GmbH & Co. KG v. Austria App no 34315/96 (ECHR, 26 February 2000)

A.D.T v United Kingdom App no 35765/97 (ECHR, 21 July 2000)

PG and JH v United Kingdom App no 44787/98 (ECHR, 25 September 2001)

Pannullo and Forte v France App no 37794/97(ECHR, 30 October 2001)

Peck v UK (2003) 36 EHRR 41; [2003] EMLR 287

Van Kück v Germany App no 35968/97 (ECHR, 12 June 2003)

Perry v United Kingdom App no. 63737/00 (ECHR, 17 July 2003)

Smirnova v Russia App nos 46133/99 and 48183/99 (ECHR, 24 July 2003)

Radio France and Others v France, App no 53984/00 (ECHR, 30 March 2004)

Plon (Societe) v France App no 58148/00 (ECHR, 18 May 2004)

Pedersen and Baadsgaard v. Denmark App no 49017/99 (ECHR, 17 December 2004, ECHR)

Von Hannover v Germany, App no 59320/00 (ECHR, 24 September 2004)

Krone Verlag GmbH & Co. KG v. Austria (No. 4) App no 72331/01(ECHR, 9 November 2006)

Dyuldin and Kislov v. Russia, App no 5968/02 (ECHR, 31 July 2007)

Cumpănă and Mazăre v. Romania, App no 12556/03 (ECHR, 15 November 2007)

A v Norway App no 28070/06 (ECHR, 9 April 2009)

Karako v Hungary App no 39311/05 (ECHR, 28 April 2009)

Pfeifer v Austria App no 24733/04 (ECHR, 17 February 2011)

Sipos v Romania App no 26125/04 (ECHR, 3 May 2011)

Mosley v UK App No. 48009/08 (ECHR, 10 May 2011)

Avram and Other v Moldova App no 41588/05 (ECHR, 5 July 2011)

Standard Verlags GmbH v Austria (No. 3) App no 34702/07 (ECHR, 10 January 2012)

Axel Springer AG v Germany App no 39954/08 (ECHR, 7 February 2012)
App nos. 40660/08 and 60641/08 w/ *Von Hannover v Germany (No.2)* (7 February 2012)

Ageyevy v Russia App no 7075/10 (*ECHR*, 18 April 2013)

Von Hannover v Germany (No.3) App no. 8772/10 (ECHR, 19 September 2013)

Delfi AS v Estonia, App no 64569/09 (ECHR, 10 October 2013)

Lillo-Stenberg and Sæther v. Norway App no 13258/09 (ECHR, 16 January 2014)

Ojala and Etukeno Oy v. Finland, App no 69939/10 (ECHR, 14 January 2014) and *Ruusunen v. Finland*, App no 73579/10 (ECHR, 14 January 2014)

Couderc and Hachette Filipacchi Associes v France, App no 40454/07 (ECHR, 12 June 2014)

Delfi AS v Estonia, App no. 64569/09 (ECHR, 16 June 2015)

Erla Hlynsdóttir v. Iceland (No. 3) App no 54145/10 (ECHR, 2 June 2015)

Egill Einarsson v Iceland App no 24703/15 (ECHR, 7 November 2017)

Faludy-Kovács v. Hungary App no 20487/13 (ECHR, 23 January 2018)

Vincent Del Campo v Spain App no 25527/13 (ECHR, 6 November 2018)

UK

Duke of Brunswick v Harmer (1950) 175 ER 441

Cohen v Daily Telegraph [1968] WLR 916

Slim and others v Daily Telegraph Ltd and others [1968] 2 W.L.R 599, 5 QB 157

Coco v AN Clark Engineers Ltd [1969] RPC 41

Woodward v Hutchins [1977] 2 All ER 751, [1977] 1 WLR 760

Malone v Commissioner of Police of the Metropolis (No2) [1979] Ch.344 [375]

Monson v Tussauds [1984] 1 QB 671

Attorney General v Guardian Newspapers Ltd (No.2) (1991) 14 EHRR 229

Telnikoff v Matusevitch [1992] 2 AC 343, [1992] UKHL 2

Derbyshire County Council v Times Newspapers and ors [1993] AC 534.

R v SoS for Home Department ex parte Simms [1999] 3 All ER 400

Reynolds v Times Newspapers Ltd [2001] 2 AC 127

Tse Wai Chun Paul v Albert Cheng [2001] EMLR 777

Theakston v MGN Limited [2002] EWHC 137, [2002] E.M.L.R 22

Douglas v Hello! Ltd (No2) [2003] EWCA Civ 139; [2003] EMLR 585

Campbell v MGN Ltd [2004] UKHL 22, [2004] 2 AC 457

Re S (a child) [2004] UKHL 47; [2005] 1 AC 593

Wainwright v Home Office [2004] 2 AC 406

A v B [2005] EMLR 36

A v B, C and D [2005] EWHC 1651 (QB); [2005] EMLR 851

Cream Holdings Ltd v Banerjee and Others [2005] 1 AC 253

Douglas v Hello! [2006] QB 125

HRH Prince of Wales v Associated Newspapers [2006] EWCA Civ 1776

McKennitt v Ash [2006] EWCA CIV 1714

Jameel (Mohammed) and another v Wall Street Journal Europe Sprl [2007] 1 AC 359 (HL)

David Murray v Express Newspapers [2007] EWHC 1908 (Ch) and [2008] EWCA Civ. 446

Max Mosley v News Group Newspapers Limited: [2008] EWHC 1777 (QB)

The Author of a Blog v Times Newspapers Ltd [2009] EWHC 1358 (QB)

British Chiropractic Association v Singh [2010] EWCA Civ 350; [2011] EMLR 1

Flood v Times Newspapers [2010] EWCA Civ 804, [2012] UKSC 11

Terry (previously "LNS") v Persons Unknown [2010] EWHC 119 (QB)

Thornton v Telegraph Media Group Ltd (No.2) [2010] EWHC 1414 (QB); [2010] EMLR 25

AMP v Persons Unknown [2011] EWHC 3454 (TCC)

CTB v News Group Newspapers Limited [2011] E.W.H.C. 1326 (QB)

Ferdinand v MGN [2011] EWHC 2454 (QB)

Goodwin v News Group Newspapers (No.3) [2011] EWHC 1437 (QB)

Hutcheson (previously "KGM") v News Group Newspapers Ltd [2011] EWCA Civ 808

K v News Group Newspapers Ltd [2011] EWCA Civ 439 [2011] 1 WLR

Carina Trimingham v Associated Newspapers Limited [2012] EWHC 1296 (QB)

Contostavlos v Mendahun [2012] EWHC 850

Jonathan Spelman (by his Litigation Friends Mark Spelman and Caroline Spelman) v Express Newspapers [2012] EWHC 355 (QB)

Sugar v BBC (and another) [2012] 1 W.L.R 439

AAA v Associated Newspapers Ltd [2013] EWCA Civ 554 (CA)

Reachlocal UK Ltd v Bennett and Ors and Mason v Huddersfield Giants Ltd [2013] EWHC 2869 (QB)

Robert Gordon Martin and Heather Elaine Martin and Ors v Gabrielle Giambrone P/A Giambrone & Law, Solicitors and European Lawyers [2013] NIQB 48

Rocknroll v News Group Newspapers Ltd [2013] EWHC 24 (Ch)

The Lord McAlpine of West Green v Sally Bercow [2013] EWHC 1342 (QB)

Weller v Associated Newspapers Ltd High Court (Queen's Bench Division) [2014] EWHC 1163 (QB), [2014] E.M.L.R. 24

Yeo MP v Times Newspapers [2014] EWHC 2853 (QB)

Ames & Another v Spamhaus Project Ltd & Another [2015] EWHC 127 (QB)

Google Inc v Judith Vidal – Hall [2015] E.M.L.R. 15, [2015] E.W.C.A. Civ 311

Economou v de Frietas [2016] EWHC 1853 (QB) [139]

Lachaux v Independent Print Ltd [2016] QB 402; [2015] EWHC 2242

PJS (Appellant) v News Group Newspapers Ltd (Respondent) [2016] UKSC 26

Jan Tomasz Serafin v Grzegorz Malkiewicz, Czas Publishers Ltd, Teresa Bazarnik-Malkiewicz [2017] EWHC 2992 (QB)

Lachaux v Independent Print Ltd [2017] EWCA Civ 1334

Monroe v Hopkins [2017] EWHC 433 (QB), [2017] W.L.R 68

Townsend v Google Inc [2017] NIQB 81

Doyle v Smith [2018] EWHC 2935 (QB)

Economou v de Frietas [2018] EWCA Civ 2591

NPV v QEL [2018] EWHC 703 (QB)

NT1 and NT2 v Google LLC (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB)

Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police [2018] EWHC 1837 (HC)

Dr Salman Butt v The Secretary of State for the Home Department [2019] EWCA Civ 933

US

Abrams v United States 250 U.S. 616 (1919)

New York Times Co. v Sullivan 376 U.S 254 (1964).

Legislation/Treaties

UK legislation

The Rehabilitation of Offenders Act 1974

The Limitation Act 1980

The Public Order Act 1986

The Data Protection Act 1998

The Human Rights Act 1998

The Defamation Act 2013

The Defamation (Operators of Websites) Regulations 2013, Statutory Instrument No.3028

The Data Protection Act 2018

The Online Harms White Paper 2019

EU Instruments

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 of the free movement of such data [1995] O.J L 281, 31.

Proposal for a Regulation of the European Parliament and of the Council on the protection of personal data and of the free movement of such data (General Data Protection Regulation) [2012] COM(2012) 11 final (25/1/12).

Directive on Copyright in the Digital Single Market [2016] COM(2016) 593 final (14/9/2016).

Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [2016] OJ L119/1 (27/4/2016).

Directive on copyright in the Digital Single Market [2016] COM(2016) 593 final (14/9/2016).

Conventions/Treaties/Charters

Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950, 3 September 1953) 005 CETS (ECHR).

Charter of Fundamental Rights of the European Union, (18/2/2000) OJ C364/3

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing European Community [2007] OJ C306/1

Memorandums, Communications, Guidelines, Reports, Press Releases

Report of the Committee on Defamation (Cmnd 5909, 1975)

House of Commons Research Paper 98/48 (17 April 1998)

Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (adopted 16 February 2010)

Joint Committee on the Draft Defamation Bill, Session 2010-2 (minutes), HL Paper 203, accessible at: https://publications.parliament.uk/pa/jt201012/jtselect/jtdefam/203/203.pdf (last accessed 3/9/18)

European Commission, MEMO/12/41, 'Data Protection Reform Explanatory Memo-Frequently Asked Questions' (25/1/12) available at; http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en (last accessed 10/4/17)

Reding V, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (22 January 2012) available at http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (last accessed 29/12/18)

Phillipson G, Memorandum to the Joint Committee on Human Rights: the Defamation Bill 2012, Executive Summary, BILLS (12-13) 066

Article 29 Data Protection Working Party, Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package, (2013) Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities

Explanatory Notes to the Defamation Act 2013, Chapter 26, available at: http://www.legislation.gov.uk/ukpga/2013/26/pdfs/ukpgaen_20130026_en.pdf (last accessed 28/3/18)

European Union Committee, EU Data Protection Law: A 'Right to be Forgotten'? (HL 2nd Report of Session 2014-2015) paper 40

Article 29 Data Protection Working Party, Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12 (26 November 2014)

Statistics Bulletin, Ministry of Justice (25 September 2014) accessible at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/358274/privacy-injunctions-statistics-january-june-2014.pdf (last accessed 13/8/19)

Article 29 Data Protection Working Party, Appendix: Core Topics in View of the Trialogue, (2015) Annex to the letters

European Commission Fact Sheet, 'Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market' (28/1/15) available at; http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (last accessed 20/6/15)

Case C-507/17 Google v CNIL, Press Release No. 2/19 (10 January 2019), accessible at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002en.pdf (last accessed 4/4/19).

Secondary Sources

Articles

Agate J, 'Battle lines drawn: privacy injunctions following CTB et al' (2011) *Entertainment Law Review* 212

Agate J, 'NPV v QEL - a familiar tale of adultery, blackmail and an interim injunction' (2018) *Entertainment Law Review* 185,186 and *NPV v QEL and ZED* [2018] EWHC 703 (QB)

Ambrose M, 'It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten' (2013) 16(2) *Stanford Technology Law Review* 369

Ambrose M. L and Ausloos J, 'The Right to be Forgotten Across the Pond' (2013) 3 *Journal of Information Law and Policy*

Anderson K and Cavallaro D, 'Parents or Pop Culture? Children's Heroes and Role Models' (2002) 78(3) *Childhood Education* 161

Auburn J, 'Implied Waiver and Adverse Inferences' (1999) 115 *Law Quarterly Review,* 590

Baker C. E, 'Giving the Audience What it Wants' (1997) 58(2) Ohio State Law Journal 311

Baker C.E, 'Realizing self – realization: Corporate Political Expenditures and Redish's Value of Free Speech' (1981) 130 *University of Pennsylvania Law Review* 646

Eric Barendt, 'Balancing Freedom of Expression and the Right to Reputation: Reflection on Reynolds and Reportage' (2012) 63(1) *Northern Ireland Legal Quarterly* 59

Bennett T, 'Why So Serious? Lachaux and the threshold of serious harm in section 1 Defamation Act 2013' (2018) *Journal of Media Law* 1

Bloustein E, 'Privacy as an aspect of human dignity: an answer to Dean Prosser' (1964) 39 *New York University Law Review* 962

Bloustein E, 'Privacy, tort law, and the constitution: is Warren and Brandeis' tort petty and unconstitutional as well?' (1968) 46(5) *Texas Law Review* 611

Bollinger L.C, 'Free Speech and Intellectual Values' (1983) 92(3) *Yale Law Journal* 438

Borghi M, Ferretti F and Karapapa S, 'Online data processing consent in EU law: a theoretical framework and empirical evidence from the UK' (2013) 21(2) *International Journal of Law and Information Technology* 109

Brennan D, 'GDPR series: personal data – an expanding concept' (2016) *Privacy & Data Protection* 12

Brimblecombe F and Phillipson G, 'Regaining Digital Privacy? The New 'Right to be Forgotten' and Online expression' 4(1) *Canadian Journal of Comparative and Contemporary Law* 1

Bulak B and Zysset A, '"Personal autonomy" and "democratic society" at the European Court of Human Rights: Friends or foes?' (2013) *UCL Journal of Law and Jurisprudence* 231

Butler O. M, ‘Confidentiality and Intrusion: building storm defences rather than trying to hold back the tide’ (2016) *The Cambridge Law Journal* 452

Charlesworth A, ‘Implementing the Union Data Protection Act 1995 in UK Law: The Data Protection Act 1998’ (1999) 16(3) *Information Law Quarterly* 204

Chlapowski F, ‘The Constitutional Protection of Informational Privacy’ (1991) 71 *Boston University Law Review* 133

Cohen J, ‘What Privacy is For’ (2013) 126 *Harvard Law Review* 1904

Costa L and Poullet Y, ‘Privacy and the Regulation of 2012’ (2012) 28 *Computer Law & Security Review* 254

Cox N, ‘Delfi AS v Estonia: The Liability of Secondary Internet Publishers for Violation of Reputational Rights under the European Convention on Human Rights’ (2014) 77(4) *Modern Law Review* 619

Danaj L and Prifti A, ‘Respect for privacy from the Strasbourg perspective’ (2012) 5 *Academicus – International Scientific Journal* 108

De Hert P and Papakonstantinou V, ‘The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals’ (2012) 28(2) *Computer Law & Security Review* 130

De Mars and O’Callaghan P, ‘Privacy and Search Engines: Forgetting or Contextualising?’ 43(2) *Journal of Law and Society* 257

De Vries S, ‘EU and ECHR: Conflict or Harmony? - Editorial’ (2013) 9(1) *Utrecht Law Review* 78

Descheemaeker E, ‘Mapping Defamation Defences’ (2015) 78 *Modern Law Review* 641

Eckes C, ‘EU Accession to the ECHR: Between Autonomy and Adaption’ (2013) 76(2) *The Modern Law Review* 254

Elwood J, ‘Outing, Privacy and the First Amendment’ (1992) 102 *Yale Law Journal* 747

Erdos D, ‘European Data Protection and Online New Media: Mind the Enforcement Gap’ (2016) 43(4) *Journal of Law and Society* 534

---- -----, “Beyond ‘Having a Domestic’? Regulatory Interpretation of European Data Protection Law and Individual Publication” (2017) 33:3 *Computer Law and Security Review* 275

----- -----, ‘Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU *acquis*’ (2018) *International Journal of Law and Information Technology* 189

Fazlioglu M, 'Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet' (2013) 3(3) *International Data Privacy Law* 149

Follesdal A and Hix S, 'Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik' (2006) 44 *Journal of Common Market Studies* 533

Fried C, 'Privacy' (1967) 77 *Yale Law Journal* 475

Gabriela G and Cerasela S. E, 'The EU General Data Protection Regulation Implications for Romanian Small or Medium-sized enterprises' (2018) XVIII *' "Ovidius" University Annals, Economic Sciences Series* 88

Gavison R, 'Privacy and the Limits of the Law' (1980) 89(3) *The Yale Law Journal* 421

Gavsion R, 'Too Early for a Requiem: Warren and Brandeis were right on privacy v free speech' (1992) 43(3) *South Carolina Law Review* 437

Gerety T, 'Redefining Privacy' (1977) 12(2) *Harvard Civil Rights – Civil Liberties* Law Review 233

Gewirtz P, 'Privacy and Speech' (2001) *The Supreme Court Review* 139

Gomery G, 'Whose autonomy matters? Reconciling the competing claims of privacy and freedom of expression' (2007) 27(3) *Legal Studies* 404

Greenawalt K, 'Free Speech Justifications' (1989) 89 *Columbia Law Review* 119

Howarth D, 'Libel: Its purpose and Reform' (2011) 74(6) *Modern Law Review* 845

Hughes D, 'Two concepts of privacy' (2015) 31 *Computer Law & Security Review* 527

Hughes K, 'Publishing Photographs Without Consent' (2014) 6(2) *Journal of Media Law* 180

------ ------, 'The Public Figure Doctrine and the Right to Privacy' (2019) 78(1) *Cambridge Law Journal* 70

Hunt C, 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort' (2011) 37(1) *Queen's Law Journal* 167

----- ------. 'Strasbourg on Privacy Injunctions' 70(3) (2011) *Cambridge Law Journal* 489

Hylton K, 'Property rules, liability rules and immunity: an application to cyberspace' (2007) 87(1) *Boston University Law Review* 1

Jarvis Thomson J, 'The Right to Privacy' (1975) 4(4) *Philosophy & Public Affairs* 295

Jouard S, 'Some Psychological Aspects of Privacy' (1966) 31 *Law & Contemporary Problems* 307

Kalvern H, ‘Privacy in tort law – were Warren and Brandeis Wrong?’ (1996) 31 *Law & Contemporary Problems* 326

Lahav P, ‘Holmes and Brandeis: Libertarian and Republican Justifications for Free Speech’ (1988) 4 *Journal of Law and Politics* 451

Lemley M, ‘Rationalizing internet safe harbors’ (2007) 6 *Journal on Telecommunications and High Technology Law* 102

Lichtman D and Posner E, ‘Holding Internet Service Providers Accountable’ (2006) 14 *The University of Chicago Supreme Court Law Review* 221

Lock T, ‘The future of the European Union's accession to the European Convention on Human Rights after Opinion 2/13: is it still possible and is it still desirable?' (2015) 11(2) *European Constitutional Law Review* 239

Manu T and Moreno F.R, ‘Is social media challenging the authority of the judiciary? Rethinking the effectiveness of anonymised and super injunctions in the age of the internet’ (2016) 18(32) *Journal of Legal Studies* 39

Marmor A, ‘What is the Right to Privacy’ (2014) 43(1) *Philosophy & Public Affairs* 3

Marsoof A, ‘Online social networking and the right to privacy: the conflicting rights of privacy and expression’ (2011) 19(2) *International Journal of Law and Information* 110

Marsoof A, ‘Online social networking and the right to privacy: the conflicting rights of privacy and expression’ (2011) 19(2) *International Journal of Law and Information* 110

Marsoof A, ‘Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression’ (2011) 19(2) *International Journal of Law and Information Technology* 110

Mathiesson S and Barendt E, ‘Carina Trimingham v Associated Newspapers: A right to ridicule?’ (2012) 4(2) *Journal of Media Law* 309, 313

Mead D, ‘A socialised conceptualisation of individual privacy: a theoretical and empirical study of the notion of the “public” in MoPI cases’ (2017) 9(1) *Journal of Media Law* 100

Mills M, ‘Sharing privately: the effect publication on social media has on expectations of privacy’ (2017) 9(1) *Journal of Media Law* 45

Mo J.Y.C, ‘Misuse of private information as a tort: The implications of Google v Judith Vidall – Hall (2017) 33 *Computer Law and Security Review* 87

Moosavian R, ‘A just balance or just imbalance? The role of metaphor in misuse of private information’ (2015) 7(2) *Journal of Media Law* 196

Moravcsik A, ‘In Defence of the ‘Democratic Deficit’: Reassessing Legitimacy in the European Union’ (2002) 40 *Journal of Common Market Studies* 603

Moreham N, 'Privacy in the Common Law' (2005) 121 *Law Quarterly Review* 628

Mullis A and Scott A, 'The swing of the pendulum: reputation, expression and the recentering of English libel law' (2012) 61(3) *Northern Ireland Legal Quarterly* 27

Mullis A and Scott A, 'Tilting at Windmills: the Defamation Act 2013' (2014) 77(1) *Modern Law Review* 87

O'Callaghan P, 'False Privacy and Information Games' (2013) 4(3) *Journal of European Tort Law* 282

O'Meara N, '"A More Secure Europe of Rights?" The European Court of Human Rights, the Court of Justice of the European Union and EU Accession to the ECHR' (2011) 12(10) *German Law Journal* 1813

Parent W.A, 'Privacy, Morality and the Law' 12(4) *Philosophy & Public Affairs* 269

Parker R, 'A Definition of Privacy' (1973) 27 *Rutgers Law Review* 275

Pavone T, 'The Past and Future Relationship of the European Court of Justice and the European Court of Human Rights: A Functional Analysis' M.A Programme in Social Sciences, University of Chicago (28th May 2012) 1

Phillipson G, 'Leveson, the Public Interest and Press Freedom' (2013) 5(2) *Journal of Media Law* 220

------ -------, 'Max Mosley goes to Strasbourg: Article 8, claimant notification and interim injunctions' (2009) 1(1) *Journal of Media Law* 73

------- -------, 'The "global pariah", the Defamation Bill and the Human Rights Act' (2012) 63(1) *Northern Ireland Legal Quarterly* 149

------ --------, 'Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726

Posner E, 'The Right of Privacy' (1978) 12 *Georgia Law Review* 393

Post R, 'Three Concepts of Privacy' (2000) 89 *The Georgetown Law* Journal 2087

Rachels J, 'Why Privacy is Important' (1975) 4(4) *Philosophy & Public Affairs* 323

Raz J, 'Free Expression and Personal Identification' (1991) 11 *Oxford Journal of Legal Studies* 303

Redish M. H, 'Self – realization, Democracy and Freedom of Expression: a reply to Professor Baker' (1982) 130 *University of Pennsylvania Law Review* 678

Redish M. H, 'The Value of Free Speech' (1982) 130 *University of Pennsylvania Law Review* 591

Reiman J, 'Privacy, Intimacy and Personhood' (1976) 6(1) *Philosophy & Public Affairs* 26

Rosen J, 'The Right to be Forgotten' (2012) *Stanford Law Review Online* 88

Rosen J, 'Why Privacy Matters' (2000) 24(4) *The Wilson Quarterly* 32

Rowbottom J, 'A landmark at a turning point: Campbell and the use of privacy law to constrain media power' (2015) 7(2) *Journal of Media Law* 170

Sartor G, 'Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?' (2013) 3(1) *International Data Privacy Law*

Sartor G, 'The Right to be Forgotten in the Draft Data Protection Regulation' (2015) 5(1) *International Data Privacy Law* 64

Schartum D.W, 'Designing and Formulating Data Protection Laws' (2010) 18(1) *International Journal of Law and Information Technology* 1

Schwartz P, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 *Harvard Law Review* 1966

Shils E, 'Privacy: its constitution and its vicissitudes' (1966) 31 Law *& Contemporary Problems* 281

Solove D, '"I've Got Nothing to Hide" and Other Common Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745

Taylor J Mark, 'Data Protection: Too Personal to Protect?' (2006) 3(1) *SCRIPT-ed* 72

Toulson R, 'Freedom of Expression and Privacy' (2007) 41 (2) *The Law Teacher* 139

Ustaran E, 'The wider effect of the "right to be forgotten" case' (2014) Privacy *& Data Protection* 8

Vechten Veeder V, 'The History and Theory of the Law of Defamation - I' (1903) 3(8) *Columbia Law Review* 546

Volokh E, 'Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People Speaking About You' (2000) 52 *Stanford Law Review* 1049

Voorhoof D, 'European Court of Human Rights: Lillo-Stenberg and Sæther v. Norway' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2014-3/1)

Voorhoof D, 'European Court of Human Rights: Standard Verlags GmbH v Austria' Iris: Legal Observations of the European Audiovisual Observatory (IRIS 2012-2/2)

Voss W. G, 'One year and loads of data later, where are we? An update on the proposed European Union General Data Protection Regulation' (2013) 16(10) *Journal of Internet Law* 13

Warren S and Brandeis L, 'The Right to Privacy' (1980) 4 *Harvard Law* Review 193

Weib W, 'Human Rights in the EU: Rethinking the Role of the European Convention on Human Rights After Lisbon' (2011) 7(1) *European Constitutional Law Review* 64

White G.E, 'The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America' (1996) 95(2) *Michigan Law Review* 299

Wragg P, 'A Freedom to Criticise? Evaluating the Public Interest in Celebrity Gossip after Mosley and Terry' (2010) 2(2) *Journal of Media Law* 295

Wragg P, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) *Journal of Media Law* 225

Wragg P, 'The benefits of privacy – invading expression' (2013) 64(2) *Northern Ireland Legal Quarterly* 187

Yoshida K, 'Privacy injunctions in the internet age – PJS' (2016) 4 *European Human Rights Law Review* 434

Zimmerman D, 'The "New" Privacy and the "Old": Is Applying the Tort Law of Privacy Like Putting High Button Shoes on the Internet?' (2012) 17 *Communications Law and Policy* 107

Žliobaitė I and Custers B, 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models' (2016) 24 *Artif Intell Law* 183

Books/theses

Ausloos J, *The Right to Erasure: safeguard for informational self-determination in a digital society?* (PhD thesis, KU Leuven, September 2018) copy on file with author

Barendt E, *Freedom of Speech* (2nd Edn, OUP 2007)

Bernal P, 'The EU, the US and the Right to be Forgotten' in Gutwirth S, Leenes R and De Hert P (Eds) *Reloading Data Protection* (Springer 2014)

Collins M, *The Law of Defamation and the Internet* (OUP 2001)

Deakin S, Johnson A and Markesinis B, *Tort Law* (6th Edn, OUP 2012)

Fellner R, *The Right to be Forgotten in the European Human Rights Regime* (GRIN Verlag GmbH 2014)

Fenwick H and Phillipson G, *Media Freedom Under the Human Rights Act* (Oxford University Press 2006)

Fenwick H, Phillipson G and Masterman M (Eds) *Judicial Reasoning Under the Human Rights Act* (Cambridge University Press 2007)

Horsey K and Rackley E, *Tort Law* (OUP 2015)

Howarth D, *Textbook on Tort* (Butterworths 1995)

Kenyon A (Ed) *Comparative Defamation and Privacy Law* (CUP 2016)

Lynskey O, *The Foundations of EU Data Protection Law* (OUP, 2015)

Mayer-Schönberger V, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009)

McLean Shiela AM, (ed) *First, Do No Harm: Law, Ethics and Heathcare* (Ashgate 2006)

Mill J.S, *On Liberty* (Cosimo Classics Philosophy 2009)

Mowbray A, *Cases and Materials on the European Convention on Human Rights* (Oxford University Press 2007)

Nissenbaum H, *Privacy in Context* (Stanford University Press 2009)

Orwell G, *Nineteen Eighty-four* (Penguin Classics 2004)

Richards N, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press 2015)

Schoeman F(ed) *Philosophical Dimensions of Privacy* (Cambridge University Press 1984)

Solove D, *The Future of Reputation* (Yale University Press 2007)

-------- ---, 'Speech, Privacy and Reputation on the Internet' in Levmore S & Nussbaum M (Eds), *The Offensive Internet* (Harvard University Press 2010)

Townend D, Rouille Mirza S, Beylveld D and Wright J (Eds), *The Data Protection Directive and Medical Research Across Europe* (Ashgate 2005)

Online News Articles /Surveys/Resources

No credited author

'83% of mobile phone users within the UK in 2018 now use a 'Smartphone', capable of connecting (and therefore sharing) information online. See the survey at *Statista*, accessible at: https://www.statista.com/statistics/387218/market-share-of-smartphone-devices-in-the-uk/ (last accessed 13/11/18)

59% of the population now have active social media accounts: see http://socialmedialondon.co.uk/digital-social-mobile-statistics-2015 (last accessed 13/4/16)

91% of 'millennials' (15-34 year olds) use the social networking site 'Facebook' as of September 2015: see http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/ (last accessed 8/4/17).

'About Public and Protected Tweets', Twitter available at: https://support.twitter.com/articles/14016 (last accessed 22/4/16)

'Defamation expert: New '1 year after publication' rule means an easy life for UK libel judges' (*The Register*, 7 January 2014) accessible at: https://www.theregister.co.uk/2014/01/07/single_publication_defamation_reform/ (last accessed 13/9/18).uk/2014/01/07/single_publication_defamation_reform/ (last accessed 13/9/18)

'Government "Call for Views" on GDPR Derogations' (*Inforrm*, 19 April 2017) accessible at: https://inforrm.wordpress.com/2017/04/19/government-consultation-on/ (last accessed 28/4/17)

'How can social media ruin a relationship' (*TheLoveQueen.com*) accessible at: https://www.thelovequeen.com/how-can-social-media-ruin-your-relationship// (last accessed 22/7/19).

'In Any Acquisition, This is What We Think Twitter Is Worth' (*Forbes*, 26 September 2016) accessible at: https://www.forbes.com/sites/greatspeculations/2016/09/26/in-any-acquisition-heres-how-much-we-think-twitter-is-worth/#559440f2649a (last accessed 28/4/17)

'Internet access – households and individuals, Great Britain: 2018', Office for National Statistics, accessible at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018 (last accessed 28/12/18).

'List of Data Breaches' accessible at: https://en.wikipedia.org/wiki/List_of_data_breaches (last accessed 13/11/18)

National Audit Office, 'Efficiency in the criminal justice system' Ministry of Justice, HC 852 Session 2015-16 (1 March 2016) accessible at: https://www.nao.org.uk/wp-content/uploads/2016/03/Efficiency-in-the-criminal-justice-system.pdf (last accessed 9/5/19)

'PCC Ruling: Twitter, Journalism and Privacy' (1st March 2011) available at: http://healthyhomenepal.com/1598-article.html (last accessed 15/10/18)

'Quora Hacked: Website Logs Out 200 Million Users', Computer Business Review (4th December 2018) accessible at: https://www.cbronline.com/news/quora-hack-100-million (last accessed 29/12/18)

'Special Eurobarometer 431' survey conducted in 2015 by the European Union Commission, investigating attitudes of Internet users to their personal data online, accessible at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (last accessed 8/4/17)

'Teacher sacked for posting picture of herself holding glass of wine and beer on Facebook' (*The Daily Mail*, 7 February 2011) accessible at: http://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html

'The Cambridge Analytica Files' *The Guardian*, accessible at: https://www.theguardian.com/news/series/cambridge-analytica-files (last accessed 29/12/18)

'The Top 20 Valuable Facebook Statistics – Updated December 2018' (*Zephoria Digital Marketing*, 28 November 2018) accessible at: https://zephoria.com/top-15-valuable-facebook-statistics/ (last accessed 29/12/18)

'Total number of Websites' (*Livestats*, June 2018) accessible at: https://www.internetlivestats.com/total-number-of-websites/ (last accessed 28/8/19).

'Viral Images that Broke the Internet' (*The Daily Express*, 31 March 2017) accessible at: http://www.express.co.uk/pictures/galleries/4523/pictures-broke-internet-viral-funny-amazing-in-pictures (last accessed 21/4/17)

Alphabetised

Ausloos J, 'European Court rules against Google, in Favour of the Right to be Forgotten' (*LSE Blogs*, 13 May 2014) (last accessed 9/7/15)

Baggs M, 'Revenge porn: what to do if you're a victim' (*BBC News*, 24 January 2018) accessible at: https://www.bbc.co.uk/news/newsbeat-42780602 (last accessed 13/11/18)

Battisby A, 'The latest UK social media statistics for 2018' (*Avocado Social*, 2 April 2018). Accessible at: https://www.avocadosocial.com/the-latest-uk-social-media-statistics-for-2018/ (last accessed 29/12/18)

------- ------ 'Social usage largely aligned across the pond, key differences: Whatsapp, Pintrest, LinkedIn' (*Avocado Social*, 2 April 2018) accessible at: https://www.avocadosocial.com/the-latest-uk-social-media-statistics-for-2018/ (last accessed 13/11/18)

Bean D, '11 Brutal Reminders That You Can and Will Get Fired for What You Post on Facebook' (*Yahoo Tech*, 6 May 2014) accessible at: https://www.yahoo.com/tech/11-brutal-reminders-that-you-can-and-will-get-fired-for-84931050659.html (last accessed 24/4/16)

Bedat A, 'Case Law, Strasbourg; Von Hannover v Germany (no.3) Glossing Over Privacy' (*Inforrm*, 13 October 2013) available at: https://inforrm.wordpress.com/2013/10/13/case-law-

strasbourg-von-hannover-v-germany-no-3-glossing-over-privacy-alexia-bedat/ (last accessed 3/2/19)

Bernal P, 'The Right to be Forgotten in the post-Snowden Era' (*Privacy in Germany*, 5 August 2014) accessible at: http://www.pingdigital.de/ce/the-right-to-be-forgotten-in-the-post-snowden-era/detail.html (last accessed 12/7/15)

----- -----, 'Are Google intentionally overreacting to the Right to be Forgotten?' (*Inforrm*, 4 July 2014) available at; https://inforrm.wordpress.com/2014/07/04/are-google-intentionally-overreacting-to-the-right-to-be-forgotten-paul-bernal/ (last accessed 8/7/15),

Birdsong T, 'Could Your Social Media History Come Back to Bite You?' (*McAffee*, 9 August 2016) accessible at: https://securingtomorrow.mcafee.com/consumer/family-safety/could-your-social-media-history-come-back-to-bite-you/ (last accessed 22/7/19)

Cain N and Carter-Coles R, 'GDPR and the Data Protection Act 2018 – how do they impact publishers?' (*RPC*, 28 May 2018) accessible at: https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/ (last accessed 14/3/19)

Callus G, 'GDPR and journalism: the new regime' (*Inforrm*, 5 June 2018) *Inforrm's Blog*, accessible at: https://inforrm.org/2018/06/05/gdpr-and-journalism-the-new-regime-greg-callus/ (last accessed 4/12/18)

Clifford C, 'Bebo founder buys back his website for $1 million and shuts it down right after' (*Entrepreneur*, 7 August 2013) accessible at: https://www.entrepreneur.com/article/227739 (last accessed 21/8/17)

Constine J, 'How Big is Facebook's Data? 2.5 Billion Pieces of Content and 500+ Terabytes Ingested Every Day' (*Techcrunch*, 22 August 2012) accessible at: https://techcrunch.com/2012/08/22/how-big-is-facebooks-data-2-5-billion-pieces-of-content-and-500-terabytes-ingested-every-day/ (last accessed 27/4/17)

Coppel QC P, 'The Data Protection Act 1998 & personal privacy', a speech for the *Statute Law Society* (19 March 2012) available at: http://www.statutelawsociety.co.uk/wp-content/uploads/2014/01/19.03.12_P.Coppel_paper.pdf (last accessed 8/4/17)

Correa D, Silva L.A, Mondal M, Benevenuto F, Gummadi K.P, 'The Many Shades of Anonymity: Characterizing Anonymous Social Media Content (2015) Association for the Advancement of Artificial Intelligence, accessible at: https://socialnetworks.mpi-sws.org/papers/anonymity_shades.pdf (last accessed 10/9/18)

Council of Europe/European Court of Human Rights, 'Information Note on the Court's case – law no. 34: P.G. and J.H. v. the United Kingdom - 44787/9 (September 2001) accessible for download at Hudoc webpage, last accessed (18/4/16)

Curtis S, 'How to permanently delete your Facebook account' (*The Daily Telegraph*, 19 August 2015) available at: http://www.telegraph.co.uk/technology/facebook/11812145/How-to-permanently-delete-your-Facebook-account.html (last accessed 17/4/16)

Eckes C, 'One Step Closer: EU Accession to the ECHR', (*UK Constitutional Law*, 2 May 2013) available at: https://ukconstitutionallaw.org/2013/05/02/christina-eckes-one-step-closer-eu-accession-to-the-echr/ (last accessed 14/4/16)

Editors' Code of Practice, Independent Press Standards Organisation, available at: https://www.ipso.co.uk/editors-code-of-practice/#Privacy (last accessed 15/10/18)

Facebook, 'Branded Content, 'Overview' accessible at: https://www.facebook.com/facebookmedia/get-started/branded-content (last accessed 23/4/18)

Facebook Investor Relations, 'Facebook Reports Fourth Quarter and Full Year 2016 Results' (*Facebook*, 1 February 2017) accessible at: https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx (last accessed 21/8/17)

Farrell H, 'Five key questions about the European Court of Justice's Google decision' (*The Washington Post: Monkey Cage,* 14 May 2014)

Garner D, 'Case Law: Economou v de Freitas, Court of Appeal guidance on "public interest" defence' (Inforrm, 5th December 2018) accessible at: https://inforrm.org/2018/12/05/case-law-economou-v-de-freitas-court-of-appeal-guidance-on-public-interest-defence-dominic-garner/ (last accessed 11/9/19)

Gotev G, Court of Justice rejects draft agreement of EU accession to ECHR' (*EurActiv,* 14 January 2015) accessible at: http://www.euractiv.com/section/justice-home-affairs/news/court-of-justice-rejects-draft-agreement-of-eu-accession-to-echr/ (last accessed 14/4/16)

Groussot X, Lock T and Pech L, 'EU accession to the European Convention on Human Rights: a Legal Assessment of the Draft Accession Agreement of the 14th October 2011' (Foundation Robert Schuman Policy Paper – European Issues, 7th November 2011 no.218) available at: http://www.robert-schuman.eu/en/doc/questions-d-europe/qe-218-en.pdf (last accessed 14/4/16)

Halliday J and Agencies, 'Jeremy Clarkson lifts 'pointless' injunction against ex-wife' (*The Guardian,* 27 October 2011) accessible at: https://www.theguardian.com/media/2011/oct/27/jeremy-clarkson-lifts-injunction?newsfeed=true (last accessed 15/10/18)

Helme I, 'Cases - Karako v Hungrary', (*OneBrickCourt.com)* accessible at https://www.onebrickcourt.com/cases.aspx?menu=main&pageid=42&caseid=212 (last accessed 7/10/2017)

Henry A, 'How You're Unknowingly Embarrassing Yourself Online (and How to Stop)' (*LifeHacker*, 5 October 2013) accessible at: http://lifehacker.com/how-youre-embarrassing-yourself-online-without-knowing-495859415 (last accessed 1/5/16)

Hooper D, Jordan B, Waite K and Murphy O, 'The New Defamation Act 2013: What difference will it really make?' *Media Law Resource Centre,* available at: http://www.medialaw.org/component/k2/item/1815-the-new-defamation-act-2013-what-difference-will-it-really-make (last accessed 13/9/18)

Hordern V, 'How do you solve a problem like special categories of data?'(*Data Protection Leader,* March 2018) accessible at: https://www.bwbllp.com/file/dpl-march-18-victoria-hordern-article-pdf (accessed 13/2/19)

Information Commissioner's Office, 'Right to restrict processing', accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/ (last accessed 15/11/18)

Information Commissioner's Office, 'Special Category Data', accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18)

Information Commissioner's Office, 'The conditions for processing', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/ (last accessed 19/4/17)

Information Commissioner's Office, 'The principles', accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last accessed 27/11/18).

Kagan N, 'Why content goes viral: what analyzing 100 million articles taught us' (*OkDork*, 21 April 2017) accessible at: http://okdork.com/why-content-goes-viral-what-analyzing-100-millions-articles-taught-us/ (last accessed 28/4/2017)

Keller D, 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation', *Social Sciences Research Network* (22 March 2017), accessible online at: https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2914684 (last accessed 11/3/19)

Larsson S, 'Images of the digital: On the European Court of Human Rights' judgment in the case of Delfi as v. Estonia' (2015) Jurista Vards (English translation) accessible at: https://portal.research.lu.se/ws/files/6062769/7855442.pdf (last accessed 2/9/19)

Lynskey O, 'Rising like a Phoenix: The "right to be forgotten" before the ECJ' (*European Law Blog*, 13 May 2014) accessible at; http://europeanlawblog.eu/?p=2351 (accessed 9/7/15).

Magee T, 'The most significant UK data breaches' (*Computer World UK,* 4 December 2018) accessible at: https://www.computerworlduk.com/galleries/data/most-significant-uk-data-breaches-3662915/ (last accessed 29/12/18)

Maldoff G, 'How the GDPR changes rules for research', (19th April 2016), *The International Association of Privacy Professionsals Online,* accessible at https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ (last accessed 6/12/18)

Mansoori S, 'Case Law: Axel Springer v Germany, Grand Chamber finds violation of Article 10' (*Inforrm*, 9 February 2012) available at: https://inforrm.wordpress.com/2012/02/09/case-law-axel-springer-v-germany-grand-chamber-finds-violation-of-article-10-sara-mansoori/ (last accessed 1/5/16)

Mayer-Schönberger V, 'Omission of search results is not a "right to be forgotten" or the end of Google' (*The Guardian Online*, 13 May 2014) accessible at;

http://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten (last accessed 12/7/15)

Mazie S, 'Why you need to get yourself a pseudonym' (*Big Think*, 28 August 2014) accessible at: http://bigthink.com/praxis/why-you-need-to-get-yourself-a-pseudonym (last accessed on 19/4/18)

Murphy M, 'Snapchat is becoming the anti – Facebook' (*Quartz*, 29 November 2017) accessible at: https://qz.com/1141464/snap-is-redesigning-snapchat-to-split-up-messages-from-friends-and-brands-snap/ (last accessed 23/4/18)

Murray A, 'New Approach to Privacy: AMP vs Persons Unknown' (*The IT Lawyer*, 20 December 2011), accessible at: http://theitlawyer.blogspot.com/2011/12/new-approach-to-privacy-amp-v-persons.html (last accessed 12/8/19)

Newell, 'Public Places, Private Lives: Balancing privacy and freedom of expression in the United Kingdom' (2014) (77th ASIS & T Annual Meeting) Available at: SSRN: http://ssrn.com/abstract=2479093 (last accessed 22/4/16)

O'Dell E, 'What is the current status of GDPR incorporation in the EU's 28 Member States?' (*Inforrm*, 8 August 2017) accessible at: https://inforrm.org/2017/08/08/what-is-the-current-status-of-gdpr-incorporation-in-the-eus-28-member-states-eoin-odell/ (last accessed 14/11/18)

Ofcom, 'The UK is now a smartphone society', reporting on technology usage in the UK, (*Ofcom*, 6 August 2015) accessible at: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/cmr-uk-2015 (last accessed 29/12/18)

Ofcom, report on the technology usage of children, Available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-use-attitudes-14/Childrens_2014_Report.pdf (last accessed 13/4/16)

Orlowski A, 'Judge bans stolen student sex pics sharing on BitTorrent' (*The Register*, 12 January 2012) accessible at: https://www.theregister.co.uk/2012/01/12/amp_bittorrent_injunction/ (last accessed 14/8/19).

Overman C, Couderc and Hachette Filipacchi Associés v. France: A New "Respect" for Private Life? (*Oxford Human Rights Hub*, 23 November 2015) accessible at: http://ohrh.law.ox.ac.uk/couderc-and-hachette-filipacchi-associes-v-france-a-new-respect-for-private-life/ (last accessed 2/7/19)

Peers S, The CJEU and the EU's accession to the ECHR: a clear and present danger to human rights protection' (*EU Law Analysis Blogspot*, 18 December 2014) accessible at: http://eulawanalysis.blogspot.co.uk/2014/12/the-cjeu-and-eus-accession-to-echr.html (last accessed 14/4/16)

Percentage of households with home computers in the United Kingdom (UK) from 1985 to 2017' (*Statista*, 2018) available at: https://www.statista.com/statistics/289191/household-penetration-of-home-computers-in-the-uk/ (last accessed 21/9/18)

Perraduin F and Mason R, 'Chuka Umunna withdraws from Labour leadership contest' (*The Guardian*, 15 May 2015) at: http://www.theguardian.com/politics/2015/may/15/chuka-umunna-withdraws-from-labour-leadership-contest (last accessed 15/12/15)

Perrin A, 'Social media usage: 2005 – 2015 – 65% of adults now use social networking sites, a nearly tenfold jump in the past decade' (*Pew Research Centre*, 8 October 2015) accessible at: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ (last accessed 14/12/15)

Press Association, 'Nearly one in 10 children gets first mobile phone by age five, says study' (*The Guardian*, 23 August 2013) accessible at: https://www.theguardian.com/money/2013/aug/23/children-first-mobile-age-five (last accessed 29/12/18)

Press Association, 'Online all the time – average British household owns 7.4 internet devices', (*The Guardian*, 9 April 2015) accessible at: https://www.theguardian.com/technology/2015/apr/09/online-all-the-time-average-british-household-owns-74-internet-devices (last accessed 28/12/18)

Rodriguez C, 'Princess Diana: Three New Documentaries Reveal More Secrets, 20 Years After Her Death' (*Forbes*, 28 July 2017) accessible at: https://www.forbes.com/sites/ceciliarodriguez/2017/07/28/princess-diana-20-years-after-her-death-three-new-documentaries-reveal-more-secrets/#138191fa1c4a (last accessed 13/7/18)

Rowe S, 'Case Law: Butt v Home Secretary, Honest Opinion Defence Clarified' (*Inforrm*, 10 July 2019) accessible at: https://inforrm.org/2019/07/10/case-law-butt-v-home-secretary-honest-opinion-defence-clarified-samuel-rowe/ (last accessed 22/8/19)

Salm L, '70% of employers are snooping candidates; social media profiles' (*CareerBuilder.com*, 15 June 2017) accessible at: https://www.careerbuilder.com/advice/social-media-survey-2017 (last accessed 22/7/19).

Silverman J, 'Ruling puts pressure on celebrity books' (*BBC News*, 14 December 2006), accessible at: http://news.bbc.co.uk/1/hi/entertainment/6181333.stm (last accessed 8/8/19).

Simpson S, 'Social media misconduct: fair dismissal over historic tweets' (*Personnel.com*, 19 January 2017) accessible at: https://www.personneltoday.com/hr/social-media-misconduct-fair-dismissal-historic-tweets/ (last accessed 22/7/19)

Sloan A, 'NT1 and NT2: forgetting past misdemeanors' (*Information Law Blog*, 14 April 2018) accessible at: http://infolawblog.com/tag/journalism-exemption/ (last accessed 27/3/19)

Smith C, '25 Interesting Drone Facts and Statistics (2019)' (*DMR*, 25 June 2019) available at: http://expandedramblings.com/index.php/drone-statistics/ (last accessed 10/4/17)

Solove D, 'What Google Must Forget: The EU Ruling on the Right to be Forgotten' (*LinkedIn*, 13 May 2014) available at; https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten (last accessed 20/9/19).

Statt N, 'Facebook confirms years-old messages are randomly coming back to haunt users' (*The Verge*, 26 November 2018) accessible at:

https://www.theverge.com/2018/11/26/18113539/facebook-messenger-old-threads-conversations-resurfacing-no-reason

Tan E, 'Samsung is first brand in UK to try out Snapchat's new sponsored animated filters' (*Campaign*, 22 December 2017) accessible at: https://www.campaignlive.co.uk/article/samsung-first-brand-uk-try-snapchats-new-sponsored-animated-filters/1453368 (last accessed 23/4/18)

Theaker J, 'Data Protection Bill – The future of the journalism exemption' (*Inforrm*, 28 November 2017) accessible at: https://inforrm.org/2017/11/28/data-protection-bill-the-future-of-the-journalistic-exemption-james-theaker/ (last accessed 4/11/18)

Tomás Gómez-Arostegui H, 'Defining "Private life" Under Article 8 of the European Convention on Human Rights by Referring to Reasonable Expectations of Privacy and Personal Choice' available at: http://www.duo.uio.no/publ/jus/2004/21399/HTGA_Thesis.pdf (last accessed 18/5/16)

Tomlinson H, The "journalism exemption" in the Data Protection Act: Part I, the Law' (*Inforrm*, 28 March 19) accessible at: https://inforrm.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc/ (last accessed 14/3/19

Wilson I and Double T, 'Business as usual? The Court of Appeal considers the threshold for bringing a libel claim in Lachaux v Independent Print Ltd' (*Inforrm*, 16 September 2016) accessible at: https://inforrm.org/2017/09/16/business-as-usual-the-court-of-appeal-considers-the-threshold-for-bringing-a-libel-claim-in-lachaux-v-independent-print-ltd-iain-wilson-and-tom-double/ (last accessed 28/4/18)

Woods L, 'The Delfi AS v Estonia judgment explained' (*LSE Media Policy Project Blog*, 16 June 2015) accessible at: https://blogs.lse.ac.uk/mediapolicyproject/2015/06/16/the-delfi-as-vs-estonia-judgement-explained/ (last accessed 2/9/19).