The Right to be Forgotten as a Fundamental Right in the UK after Brexit

Stergios Aidinlis[*]

(2020) 25(2) Communications Law forthcoming

Abstract - Will Brexit diminish digital rights protection in the UK or are domestic institutions better-placed to deliver such protection unencumbered by the oversight of EU institutions? This article scrutinises the validity of conflicting arguments about the future of human rights protection in the UK by reference to a paradigmatically 'European' digital right, the right to be forgotten (RTBF). Having considered the interplay between the multiple layers of UK law that an RTBF claim involves, the article argues that some legal implications of Brexit will have a graver impact on digital rights protection than others. In respect of EU law no longer being supreme in the UK, the analysis offered here calls for more nuance in critical arguments about losing fundamental protections when it comes to the RTBF. Brexit, however, will erode the protection of the RTBF in the longer term as a result of the loss of EU law's direct effect. The scope of the 'British RTBF' will be gradually developed as 'narrower' compared to EU member states due to fundamental differences between the UK and European conceptions of privacy. The central place of 'reasonable expectations' of the data subject within the UK privacy conception, it is argued, sits at odds with social realities related to the RTBF and, thus, raises significant risks for the robust protection of the right in the future.

Keywords: digital rights, right to be forgotten, Brexit, fundamental rights, reasonable expectations of privacy

[*] DPhil Candidate, Faculty of Law, University of Oxford. The author acknowledges funding from the Onassis Foundation - Scholarship ID: F ZL 003-2/2017-2018 and is grateful to participants in the 2019 Information Law and Policy Centre (IALS, London) Conference on 'Digital Rights after Brexit' for advice and feedback on an earlier version of this work. The usual disclaimers apply.

1. Introduction

Ever since the landmark judgment of the Court of Justice of the European Union (CJEU) in the *Google Spain* case,[1] the so-called 'right to be forgotten' (hereafter 'RTBF'), ie de-referenced from a list of Internet search engine results, has been gaining significant traction in legal discourse.[2] Six years after *Google Spain,* this novel digital right has clearly surpassed its modest origins as a statutory data subject right 'to erasure', as it was envisaged under the previous EU Data Protection Directive.[3] Through judicial creation and interpretation, the right has now matured as a *fundamental* right, that is to be balanced against 'other fundamental rights' such as the rights to data protection, privacy, and the freedom of expression of both the publisher and the public.[4]

Google Spain has been very influential in shaping the reasoning of international and domestic courts which have tried to strike a balance between a claim to de-list information that relates to particular individuals from search engine results and the freedom of expression. The European Court of Human Rights (ECtHR) recently relied on the CJEU judgment in fleshing out its own criteria for balancing the RTBF with the 'public's right to be informed about past events and contemporary history (…) through

[1] Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] All ER (D) 124.

[2] Eg Y Padova, 'Is the right to be forgotten a universal, regional, or "glocal" right? (2019) 9(1) IDPL 15; P Lambert, 'The right to be forgotten: context and the problem of time' (2019) 24(2) Comms L 74; E Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Protección de Datos' (2014) 14(4) HRLR 761. Note that right to be forgotten claims can be either about de-listing certain items from search engine results, or about full erasure of content about an individual on the Internet, or both. The present article focuses on de-listing cases as the paradigmatic examples of a right to be forgotten claim against a search engine.

[3] Arts 6, 12 and 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC) OJ 1995 L 281, 31.

[4] Case C-507/17 *Google v Commission nationale de l'informatique et des libertés (CNIL)* [2020] 1 CMLR 24 at 45.

the use of digital press archives'.[5] In 2018, the High Court of England and Wales elaborated on the same balancing exercise in *NT1 / NT2,* articulating a set of relevant criteria to determine when does a 'reasonable expectation' of privacy outweigh expression rights.[6]

The common thread in the incremental development of the RTBF as a fundamental right in the UK lies in the application of EU law, mainly the pre-GDPR data protection directive, and the EU Charter of Fundamental Rights. As the UK has very recently embarked on its departure from the EU, however, the European Convention on Human Rights (ECHR) and common law will remain as the main sources of human rights law.[7] What are, then, the implications of Brexit for the protection of the RTBF in the UK?

The present article engages with this question, placing the RTBF, as a paradigmatic digital right, in the broader context of legal debates about human rights protection after Brexit. I argue that not all Brexit-related losses are equally grave. More specifically, the protection of the RTBF as a fundamental right will not be substantially diminished in the short term after Brexit, even if EU law will no longer be *supreme*. Even if losing the remedy of disapplication is considerable, an adequately comprehensive and protective legal and institutional framework will continue to be applicable. Longer term implications, however, are to be anticipated in the absence of EU law's *direct effect*. The scope of the RTBF will be gradually developed as narrower in the UK compared to EU Member States, as the UK tort of misuse of private information will progressively underpin more and more areas of digital privacy. The central place of 'reasonable expectations' of the data subject within the UK privacy tort, it will be argued, sits at odds with social realities related to the RTBF and, thus, raises significant risks for the robust protection of the right in the future.

---

[5] *M.L. and W.W. v Germany* Appnos 60798/10 and 65599/10 (ECtHR 2018) at 104.

[6] *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB), [2018] 3 All ER 581 at 105 et seq.

[7] N Bamforth and P Leyland, 'Public Law in a Multi-layered Constitution' in N Bamforth and P Leyland (eds),
Public Law in a Multi-layered Constitution (Hart 2003) 1-10.

To support this argument, I first draw on the broader legal disagreements on the impact of Brexit on fundamental rights and then outline the applicable legal framework for the protection of the RTBF in the UK after the latter's departure from the EU. This is followed by an analysis of the implications of Brexit for the RTBF, by reference to the two central EU law principles of *supremacy* and *direct effect*. The article concludes with a critical assessment of these implications and suggestions for future legal research into digital rights protection in post-Brexit UK.

2. Losing 'fundamentals' or bringing digital rights home?

Concerns about the impact of Brexit on the protection of the RTBF in the UK can be significantly illuminated by being considered within the broader discourse about human rights protection in post-Brexit UK, including the more 'mature' right to privacy and the right to data protection. This is neither to say that privacy protection is the exclusive purpose of the RTBF,[8] nor that privacy-related harms are necessary for an RTBF violation. Nonetheless, the RTBF has been prominently exercised as a vehicle to combat unprecedented privacy threats[9] and data protection legislation as a whole has been construed as principally aiming to protect privacy rights of data subjects.[10] In practice, beyond its statutory footing in domestic legislation like the Data Protection Act 2018 (DPA 2018),[11] an RTBF claim will often engage human rights law through the application of some form of balancing exercise between privacy and the freedom of expression.

---

[8] V Mayer-Schoenberger, *Delete: The Virtue of Forgetting in The Digital Age* (Princeton University Press 2009) 108.

[9] W Li, 'A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation' (2018) 8(4) IDPL 309, 312.

[10] Supra n 1 at 3: 'Directive 95/46 which, according to Article 1, has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of
personal data, and of removing obstacles to the free flow of such data'.

[11] S 100 of the Data Protection Act 2018: the right to 'rectification and erasure'.

Before Brexit, human rights norms in the UK stemmed from three sources: the ECHR, EU law (mainly the European Union Charter of Fundamental Rights) and common law rights.[12] This multi-layered nature of UK human rights law has created significant tensions between commentators and legal actors with regard to the desirable balance and relationships between the different legal sources.[13] These tensions become very topical in the light of one of the three sources, ie EU law, having been removed from the picture very recently.

On the one end of the spectrum, there have been those who express concern about the impact of Brexit on rights protection, stressing the risk of losing fundamental protections. Some commentators stress the 'gap' that will be left in the British 'human rights constitution' by the deliberate decision of the UK parliament, as reflected in section 5(4) of the European Union (Withdrawal) Act 2018, *not* to retain the EU Charter of Fundamental Rights (hereafter 'the Charter') in UK law.[14] Bogdanor highlights the strong legal 'bite' provided by the Charter, ie the remedy of disapplying domestic legislation that is held to be conflicting with EU law rights,[15] comparing it favourably to the 'weaker' declaration of incompatibility under the Convention framework.[16] To him, the removal of this 'hierarchically stronger' source of human rights protection is tantamount to an abolishment of fundamental rights.[17] Frantziou concurs that the removal of the Charter creates 'constitutional ambiguity' and threatens legal certainty by dismantling an existing codified framework of fundamental rights in the UK legal

[12] Supra n 7.

[13] M Elliott and K Hughes, *Common Law Constitutional Rights* (Hart 2020); R Clayton, 'The Empire Strikes Back: common law rights and the Human Rights Act' (2015) PL 6.

[14] V Bogdanor, 'Brexit and our unprotected constitution' (Constitution Society 2018); E Frantziou, 'Farewell to the EU Charter of Fundamental Rights? The Withdrawal Act and the Danger of Losing 'Fundamentals' (UCL Brexit Blog 2018).

[15] As first performed by the Employment Appeals Tribunal in *Benkharbouche v Embassy of Sudan* [2013] 10 WLUK 168.

[16] Bogdanor supra n 14 at 17.

[17] *Ibid* 18.

order.[18] Crucially, she calls attention to the loss of the 'fundamental' character of the rights, from a constitutional law perspective, warning about the essential shift of their status from foundational premises of our legal polity to the subject of everyday, informal political decisions 'in the daily agenda of Westminster'.[19]

Beyond the overarching constitutional 'gap', Kennedy and Horne highlight the relevance of removing the Charter from UK law for digital rights protection.[20] While comparing the Charter with the ECHR, they claim that the 'right to protection of personal data' under article 8 EUCFR is a 'more extensive' right than the right to private life under article 8 ECHR.[21] This claim is in line with other scholarly arguments which have pointed out that the two rights are conceptually distinct; an excessive unlawful processing of personal data may suffice for a violation of article 8 EUCFR but not necessarily for one of article 8 ECHR.[22] Stressing that the CJEU has also played a particularly pivotal role in the robust protection of digital rights, Kennedy and Horne conclude that the post-Brexit period will be associated with 'serious legal uncertainty' and 'substantive diminution of rights protections'.[23]

On the other end of the spectrum, there is more optimism that a renewed emphasis on domestic institutions can bolster the legitimacy of human rights law without sacrificing the rigour of protection. This optimism stems from a critical stance towards the so-called 'overreach' of international and European human rights law.[24] The idea of 'overreach' hints at the proper institutional balance of democratic decision-making, criticising the expanding scope and substance of judicially-administered human rights

[18] Frantziou supra n 14.

[19] Ibid.

[20] H Kennedy and A Horne, 'Rights after Brexit: some challenges ahead?' (2019) 5 EHRLR 457.

[21] Ibid 459.

[22] J Kokott and C Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) IDPL 222.

[23] Supra n 20 at 458.

[24] Eg R Ekins, 'Human Rights and the Separation of Powers' (2015) 34(2) UQLJ 217.

law over the last decades at the expense of decisions by representative political bodies.[25] Lord Sumption's 2019 Reith Lectures for the BBC exemplify this critical attitude in the UK context.[26] Sumption lamented the 'massive expansion' of the role of the British courts in determining the lawfulness of executive action on the basis of the ECHR, essentially resulting in 'unelected' European judges usurping decision-making powers from domestic legislators.[27] Entrenching 'fundamental' rights in constitutional documents, according to him, is very problematic due to the removal of 'essentially political' and contested issues from political processes and democratic input.[28]

This line of argument is sympathetic to the conservative party's long-standing commitment to 'bring rights home' by repealing the Human Rights Act (HRA) 1998 and introducing a British bill of rights.[29] Furthermore, confidence in the capacity of the common law to operate as a potent vehicle for rights protection has also been renewed in the light of a recent set of UK Supreme Court (UKSC) judgments which have been framed as the 'resurgence' of common law constitutionalism.[30] In these cases, the Court shifted attention towards common law rights as the 'natural starting point' in any legal dispute,[31] chastising litigants for their tendency to focus on the Convention as the legal basis for their claims. The common law, the Court stressed time and again, will more often than not provide an essentially similar level of protection, and is not to be treated as less protective than the ECHR.[32]

[25] C O'Cinneide, 'Rights under pressure' (2017) 1 EHRLR 43.

[26] BBC, 'The Reith Lectures, 2019: Jonathan Sumption' (June 2019).

[27] Ibid.

[28] H Kennedy and J Sumption, 'Are our human rights laws working?' (Prospect Magazine 2019).

[29] A Young and S Dimelow, '"Common sense" or Confusion? The Human Rights Act and the Conservative Party' (The Constitution Society 2015).

[30] M Elliott, 'Beyond the European Convention: Human Rights and the Common Law' (2015) 68(1) CLP 85, 92.

[31] *Kennedy v Information Commissioner* [2014] UKSC 20 at 46 (per Lord Mance).

[32] *Reilly's Application for Judicial Review, Re* [2013] UKSC 61 at 56 (per Lord Reed).

Although sceptics have largely focused on the ECHR instead of the relatively more recent framework of EU law human rights, the core of the case against supranational human rights protection is directly applicable to the question of digital rights protection, such as the RTBF, after Brexit. The removal of the EU Charter from the UK legal order will result in domestic institutions exercising more ownership of the future development of the RTBF in the UK. Will, then, the country's departure from the EU lead to a substantive diminution of the right's protection or will it signify a rejuvenation of such protection by better-placed domestic institutions?

3. The RTBF in UK law post-Brexit

To assess the implications of Brexit for the protection of the RTBF in the UK, it is important to first clarify the applicable legal framework. This section distinguishes between three different dimensions of legal protection: protective frameworks, judicial application and regulatory/enforcement capabilities. The three dimensions are analysed in turn.

i. Protective frameworks

While the RTBF's origins are to be found in the CJEU's judgment in *Google Spain*,[33] the advent of Brexit sees the existence of three protective frameworks for the right in the UK legal order: statutory data protection legislation, human rights and tort law.

Several legislative initiatives have been recently adopted to ensure that 'very little will change in data protection law in the short term in the UK'.[34] Among them, the DPA 2018, which has effectively implemented the EU GDPR into UK law, is central. Section 100 of the DPA 2018 enshrines the right to 'rectification and erasure', effectively

[33] Supra n 1.

[34] Eg s 71(1) withdrawal act & Data Protection, Privacy and Electronic Communications (EU Exit) Regulations 2019; see O Butler, 'The implications of a ''no-deal'' Brexit for data protection in the United Kingdom' (2019) 3(1) JDPP 8-20.

implementing the 'right to erasure' under article 17(1) of the GDPR. Data subjects can exercise this right to demand that a data controller, in this case a search engine,[35] erases personal data that is inaccurate, not 'relevant' or unnecessary for the purpose for which it is processed.[36] Crucially, the DPA establishes a number of exceptions to the right, when eg processing is necessary for exercising the freedom of expression and information,[37] or when the exercise of the right to erasure would make impossible or seriously impair the aims of processing for scientific or historical research purposes.[38] These exceptions hint at the need to reconcile a subject's right to be de-referenced from the results of a search engine with other legitimate aims of data processing in the public interest.

Human rights law, ie the ECHR which is implemented into UK law via the HRA 1998, offers the conceptual framework for this reconciliation. In its case law under articles 8 (right to private life) and 10 (freedom of expression) ECHR, the ECtHR has attempted to reconcile free expression with the right of individuals 'deserving of redemption (…) to escape their past mistakes'.[39] While the Strasbourg court has been criticised as unclear, inconsistent and confusing in its balancing of privacy and expression,[40] it has offered significant considerations about erasing sensitive content on the Internet. In *Tamiz v UK,* it established the reachability of a given piece of content as a crucial criterion that can decide the balance between privacy and expression.[41] When information is only accessible through a newspaper's website, for example, the Court

[35] Supra n 1 at 32-41 on search engines as data controllers.

[36] S(s) 87-89 DPA 2018.

[37] S 174 DPA 2018 and art 85 GDPR.

[38] M Mourby, H Gowans, S Aidinlis, H Smith and J Kaye, 'Governance of academic research data under the GDPR—lessons from the UK' (2019) 9(3) IDPL 192.

[39] S Wechsler, 'The Right to Remember: The European Convention on Human Rights and the Right to be Forgotten' (2015) 49(1) Colum J L & Soc Probs 135, 159.

[40] S Smet, 'Freedom of Expression and the Right to Reputation: Human Rights in Conflict' (2010) 26(1) Am U Int'l L Rev 183, 187; T Aplin and J Bosland, 'The Uncertain Landscape of Article 8 of the ECHR: The Protection of Reputation as a Fundamental Human Right?' in A Kenyon (ed), *Comparative Defamation and Privacy Law* (CUP 2016) 265.

[41] *Tamiz v United Kingdom* (2018) EMLR 6.

held that erasing it would be a disproportionate limitation of the freedom of expression under article 10.[42] By contrast, the publication of a photograph on a public Instagram profile was found to have violated the right to private life under article 8 due to the very high number of people it could potentially reach.[43]

Although an RTBF case against the UK has not yet reached Strasbourg, ECtHR judgments must generally be 'taken into account' by British courts when the latter consider claims involving Convention rights.[44] A recent case, *M.L. and W.W. v Germany,*[45] prompted the ECtHR to deal explicitly with the RTBF. In this case, the personal details of the applicants were leading, through a search on an Internet engine, to the archives of a radio station that reported the contents of a court decision that convicted them to life-long imprisonment for the murder of a famous German actor in 2000.[46] The applicants had resisted their guilt in all of the proceedings and attempted to have their convictions quashed, ultimately being released in 2007 and 2008.[47] After failing to have their personal details removed from the website of the radio station in domestic proceedings, the applicants complained to the ECtHR that, eighteen (18) years after the trial, their personal details must be erased because they are 'causing prejudice to the personal enjoyment of their right to respect for private life'.[48] Strasbourg was, ultimately, unconvinced that the German courts had overstepped their margin of appreciation in balancing the right of applicants to private life and the freedom of expression of the search engine, the radio station and the general public. Seeing no reason to contest the finding of the German courts in favour of the freedom of expression, the ECtHR highlighted the significance of the right of the public to be

[42] *Wegrzynowski and Smolczewski v Poland* Appno 33846/07 (ECtHR 2013).

[43] *Egill Einarson v Iceland* Appno 24703/15 (ECtHR 2018).

[44] S 2 of the HRA 1998.

[45] Supra n 5.

[46] Ibid at 7.

[47] Ibid at 18.

[48] Ibid at 88.

informed about significant past events and conduct historical research on them through Internet archives.[49]

The Strasbourg Court's judgment outlines a principled framework of balancing the RTBF, as a facet of the 'fundamental right to protection of personal data' under article 8,[50] with the freedom of expression under article 10 ECHR. The Court applied in the RTBF context its general privacy-expression balancing rule about the lack of a 'presumptive priority' between the two rights.[51] Balancing is to be performed on a case-by-case basis, in accordance with a set of criteria: whether the publication contributes to a debate of public interest, whether the applicant is a well-known individual, the applicant's prior conduct, as well as the content, the form and the consequences of the particular publication.[52] Although the analysis derived solely from article 8 ECHR, the judgment of the CJEU in *Google Spain* was extensively discussed as a benchmark of protection.[53]

Finally, yet importantly, recent developments indicate that the RTBF will be encompassed within the 'expanding' boundaries of the privacy-protecting tort at common law.[54] The tort of 'misuse of private information', originally stemming from the common law of confidentiality,[55] prohibits disclosure of information about a claimant that ought to have been kept secret. Crucially, to enjoy legal protection under the privacy tort, the claimant must have a 'reasonable expectation of privacy in respect of the information in question'.[56] While this is not an over-arching, all-embracing cause of

---

[49] Ibid at 101-115.

[50] *Satakunnan Markkinapörssi Oy v Finland* (2018) 66 EHRR 8 at 74.

[51] I Cram, 'The right to respect for private life: digital challenges, a comparative-law perspective. The United Kingdom' (EPRS 2018) viii.

[52] Supra n 5 at 97 et seq.

[53] Ibid at 59-63.

[54] Supra n 51 at ix.

[55] *PJS v News Group Newspapers Ltd* [2016] UKSC 26 at 25 (per Lord Mance).

[56] Supra n 6 at 42 (per Warby J); *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22 at 22 (per Lord Nicholls).

action for privacy invasions, it has been expanding to cover a wide array of privacy-related interests,[57] and has recently been used as a cause of action for the protection of the RTBF.[58] The next section of this article elaborates on the significance of the privacy tort in the development of the RTBF as a fundamental right in post-Brexit UK. Before that, however, I turn to how the discussed protective frameworks will be applied in judicial review.

ii. Judicial application

'Retained' EU law in the UK includes the judgments of the CJEU, as long as they are not effectively repealed by domestic legislation or precedent.[59] In the case of the RTBF, the recent judgment of the High Court of England and Wales in *NT1/NT2* provides sufficient confidence that the *Google Spain* principles will significantly influence the reasoning of domestic courts in the foreseeable future. In this case, the claimants sought to erase hyperlinks leading to media reports of their previous convictions from Google search results.[60] Warby J heavily relied on the *Google Spain* principles, which he described as the 'new law pronounced by the CJEU',[61] in balancing the privacy interests of the claimants with the countervailing expression interests of the publisher, the search engine and the wider public.

Warby J read the principles as suggesting that no presumptive priority is to be accorded to either privacy or expression interests *a priori*, with the outcome of a balancing exercise between fundamental rights of the same rank being contingent on the circumstances of the particular case.[62] This reading is consistent both with

[57] Eg the right to remain anonymous as a suspect of criminal proceedings in *Richard v BBC* [2018] 3 WLR 1715.

[58] Supra n 6.

[59] S(s) 2-3 of the European Union (Withdrawal) Act 2018.

[60] Supra n 6 at 5-12.

[61] Ibid at 64.

[62] Ibid at 34-37.

Strasbourg jurisprudence, as previously discussed, and domestic precedent.[63] A set of key considerations inform this balancing exercise: the nature of the information in question, ie its present-day relevance, accuracy and sensitivity for the data subject's private life, as well as the interest of the public in having this information based on the role played by the data subject in public life.[64] If there is a 'preponderant interest' of the general public in having access to the information, this would justify an interference with the privacy interests of the claimants.[65] Although the outcome of the exercise will be largely context-specific,[66] judicial review is not likely to substantially depart from the *Google Spain* principles given the latitude for interpretation and balancing those principles allow. Hence, both the RTBF protective norms and their judicial application will seemingly not alter radically in the post-exit era. That being said, will the practical ability of right-holders to effectively bring forward RTBF claims also be unaffected?

iii. Regulatory and enforcement capabilities

The process of bringing forth an RTBF claim seems substantially similar *before* and *after* Brexit. The Information Commissioner's Office (ICO) remains the responsible body for monitoring organisational compliance with the RTBF, receiving appeals against search engine decisions on first-instance requests to erase data and imposing fines for enforcement purposes.[67] Unless a request is 'manifestly unfounded' or 'excessive',

[63] *S (A Child) (Identification: Restrictions on Publication), Re* [2004] UKHL 47 at 17 (per Lord Steyn): '(…) neither article has as such precedence over the other (…) an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary'.

[64] Supra n 6 at 135 et seq.

[65] Ibid at 134.

[66] Consider eg the different outcomes in *NT1/2,* supra n 6, due to one of the applicants playing a more limited role in public life and demonstrating genuine remorse.

[67] S De Schrijver, 'The Right To Be Forgotten: The Current And Future Legal Framework' (ExpertGuides 2017).

organisations will still not be able to charge data subjects for handling a request for erasure, whereas the same time limits for compliance will apply.[68]

Based on the adoption of the *Google Spain* principles in *NT1/NT2,* claimants will need to establish the factual basis of their claim and the application of the right,[69] without needing to prove that they suffered a particular type of 'damage' or harm to their privacy. Furthermore, the burden of proof with regard to the 'relevance' and 'excessiveness' of information will remain with the defendant company.[70] Thus, consistently with the GDPR, search engines will have to demonstrate 'compelling legitimate grounds for the processing'.[71] Having provided this overview of the applicable legal framework, I now turn to my analysis of the impact of Brexit on the protection of the RTBF in the UK.

4. The Implications of Brexit for the 'British' RTBF

If significant elements of the existing EU legal protective regime for the RTBF will be retained, at least for the foreseeable future, what is really lost after Brexit? While the *Google Spain* principles or the ability of a claimant to overturn a decision by a search engine may not be affected, the UK's departure from the EU fundamentally alters the application of constitutional EU legal principles to the protection of digital rights. More specifically, I will be discussing the implications of Brexit for a 'British' RTBF by reference to the two fundamental EU law principles of *supremacy* and *direct effect*. By *supremacy*, I am referring to the normative precedence of EU law over both national law, both at the European and national levels.[72] *Direct effect* refers to the ability of

[68] Information Commissioner's Office, 'Right to erasure' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/> (visited on 9 March 2020).

[69] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR' (2 December 2019) 8.

[70] Ibid.

[71] Ibid.

[72] Case 6/64, *Costa v Ente Nazionale per l'Energia Elettrica (ENEL)* [1968] CMLR 267.

individuals to directly invoke EU law before national and European courts, independent of national implementation.[73]

The two principles aim to ensure the effectiveness and applicability of EU law and are often considered together since eg their joint application mandates national courts to 'disapply' domestic law that diverges from Union law provisions.[74] For present purposes, however, supremacy and direct effect are dissociable. As it will be argued, the loss of direct effect will influence the progressive development of the right more profoundly than the loss of supremacy. In the longer term, this will result in the development of a 'narrower' RTBF underpinned by the conceptual structure of the UK tort of misuse of private information. I discuss both, before elaborating on why this development is concerning from a digital rights perspective.

i. The loss of supremacy: beyond disapplication?

With EU law no longer being supreme within the UK legal order, there is, no doubt, much to lament in the loss of the remedy of disapplication. In the post-exit era, it is no longer possible to challenge UK legislation based on non-compliance with primary (as in the EUCFR) or secondary (as in the GDPR) EU law.

In the particular context of protecting digital rights, UK courts had developed a robust approach to assessing the conformity of domestic statutory legislation with the rights to privacy and data protection under articles 7 and 8 of the EUCFR. Following the *Benkharbouche* precedent on the horizontal applicability of EU law fundamental rights,[75] the Court of Appeal disapplied in *Vidal-Hall* section 13(2) of the previous Data

[73] Case 26-62, *Van Gend en Loos v Nederlandse Administratie der Belastingen* [1964] CMLR 423.

[74] F Fabbrini, 'After the OMT Case: The Supremacy of EU Law as the Guarantee of the Equality of the Member States' (2015) 16(4) GLJ 1003.

[75] *Benkharbouche v Secretary of State for Foreign and Commonwealth Affairs* [2017] UKSC 62 at 78 (per Lord Sumption): 'a conflict between EU law and English domestic law must be resolved in favour of the former, and the latter must be disapplied'.

Protection Act 1998 for non-conformity with the rights guaranteed by the EUCFR.[76] More specifically, the 1998 Act confined remedies for privacy intrusions to cases where pecuniary damage could be established. This was deemed by the Court as too restrictive. In *Watson,* the same Court held that significant parts of the Data Retention and Investigatory Powers Act (DRIPA) 2014 were unlawful.[77] DRIPA allowed a massive scale of data retention and surveillance for crime prevention purposes and this was found to breach articles 7, 8 and 11 EUCFR.

Are, then, the warnings that Brexit will result in an 'abolishment' of fundamental rights justified?[78] It is true that the loss of disapplication will result in a weakening of the 'legal bite' of digital rights. Disapplication as a remedy makes a particular right more 'resilient' from a constitutional perspective against legislation or administrative action that interferes with it.[79] Bogdanor, in that regard, accurately presents the EU Charter as hierarchically stronger than the ECHR or common law rights. With the Convention, UK courts may issue a 'declaration of incompatibility' under s. 4 of the HRA 1998, whereas common law statutory construction involves a reading of the relevant legislation as compatible with fundamental rights.[80] In both cases, the judiciary does not have the final word.

Yet, to equate the loss of disapplication with a loss of fundamental rights *tout court* would be to throw the baby out with the bathwater. As Elliott has argued, there is a number of vectors by reference to which the nature of human rights law protection can be 'measured'.[81] Beyond the strength of the available remedies, Elliott draws attention to the 'normative reach' of human rights, as well as the 'protective rigour' with which

[76] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311.

[77] *Secretary of State for the Home Department v Watson* [2018] EWCA Civ 70.

[78] Bogdanor supra n 14 at 7.

[79] Supra n 30 at 88.

[80] M Fordham and T de la Mare, 'Anxious Scrutiny, the Principle of Legality and the Human Rights Act' (2000) 5 JR 40

[81] Supra n 30 at 85.

courts uphold them.[82] 'Normative reach' refers to the range of protected rights and their substantive content, whereas 'protective rigour' relates to how robustly judicial review scrutinises executive action, regardless of the particular style of review (eg proportionality or reasonableness). As previously demonstrated, the provisions of the GDPR and the *Google Spain* principles that are relevant to the RTBF will continue to apply in the UK. This is due to either domestic legislation (the DPA 2018) or the obligations of the UK to follow ECtHR jurisprudence on the RTBF which is substantially consistent with *Google Spain*.[83] Crucially, it has also been argued that it is quite unlikely that the UK will renege on its obligations to adequately protect digital rights for reasons of preserving unobstructed data flows with the EU.[84] A high level of data protection is required for an 'adequacy' decision under article 45 GDPR and the UK has already made considerable progress to ensure that data flows with the EU and third countries with EU adequacy decisions will be maintained.[85]

Could Brexit, though, mean that the same legal principles will start to be applied by the courts in a less 'rigorous' manner? There do not seem to be sufficient reasons for believing this. Essentially, both before and after Brexit, the courts have been tasked with the identification of an 'acceptable balance between protecting the right to privacy and that of the public to know'.[86] One could object here that even if the *Google Spain* criteria specifying this balancing exercise in the RTBF context are retained, it was the CJEU, not domestic courts, which robustly asserted that data subjects' rights 'override, as a rule (…) the interest of the general public' in accessing information through an Internet search.[87] Unencumbered by the CJEU's supervisory authority, the objection would stress, domestic courts would accord less weight to the RTBF.

---

[82] Ibid.

[83] Supra 3/i-ii.

[84] Butler supra n 34.

[85] Ibid at 10.

[86] P Giliker, 'A Common Law Tort of Privacy? The Challenges of Developing a Human Rights Tort' (2015) 27 SAcLJ 761, 763.

[87] Supra n 1 at 97.

It is important, however, not to read too much into the CJEU's rhetorical flourish in *Google Spain*. The Article 29 Working Party clarified in its guidance on the implementation of the decision that the case law of the ECtHR, where no presumptive priority between privacy and expression is being accepted, 'matters' in determining the balance.[88] In *Manni,* the CJEU itself followed this principle of not according a presumptive priority to privacy when it held that the applicants do not have the right to erase identifiable data which was in the public register after a 'certain period of time from the dissolution of the company concerned'.[89] This is consistent with Warby J's reading of the *Google Spain* ruling in *NT1/NT2,* where he took the CJEU to be suggesting that privacy overriding expression is the most likely outcome of RTBF cases in practice, rather than a statement about the former's normative priority over the latter.[90] As in other countries where EU law will still apply,[91] UK courts will consider both expression and privacy interests and balance them according to the circumstances of each case. Hence, and as the previous analysis of the applicable legal framework to the RTBF after Brexit indicates, the 'gaps' in the UK constitution are going to be less dramatic in respect of other vectors of comparison. Does this mean, then, that worries about the implications of Brexit for the protection of digital rights are overstated?

ii. The loss of direct effect: towards a 'narrower' RTBF

After Brexit, EU legal provisions are no longer directly invokable by natural and legal persons in the UK. Like the loss of supremacy, the loss of direct effect generates short-term implications. The already analysed remedy of disapplication relied on both supremacy and direct effect of EU law. The absence of direct effect, however, also triggers longer-term repercussions, which might take time to become apparent, but are potentially quite significant and concerning from a digital rights perspective. As it will

[88] Supra n 69 at 9.

[89] Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Manni* [2017] 3 CMLR 18 at 56.

[90] Supra n 6.

[91] See S Kulk and F Borgesius, 'Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe' in J Polonetsky, O Tene and E Selinger (eds), *Cambridge Handbook of Consumer Privacy* (CUP 2017) 301.

be argued here, the increasingly stronger underpinning of the RTBF by the UK tort of misuse of private information, as opposed to the concept of privacy in European human rights law,[92] will result in a 'narrower' right, with a more limited scope and higher threshold of applicability.

More specifically, the legal conceptions of privacy are strikingly different in European and UK human rights law. To start with the European conception, it is fair to associate the development of the 'right to private life' under article 8 ECHR with continental constitutional traditions that enshrine broad and open-ended individual rights to personal autonomy. For example, Article 2 of the German Basic Law establishes the individual right to 'free development of (…) personality' as long as the right holder does not violate the rights and freedoms of others.[93] Originally interpreted as a 'negative' right to 'be let alone',[94] the right to private life incrementally matured as a 'positive freedom to control (…) personal information, engage in reputation management, and to develop one's identity and personality'.[95] The ECtHR has deliberately avoided providing an exhaustive definition of privacy-related interests protected under article 8, relying on general terms like 'personality', 'autonomy' and 'identity'.[96]

In the, relevant to the RTBF, context of personal information, the European notion of privacy is similarly under-determinate and 'open to a range of plausible

[92] 'European' is used here to reflect the substantive similarity of the privacy right in the ECHR and the EU Charter, in light of art 52(3) of the latter: '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. This provision shall not prevent Union law providing more extensive protection'.

[93] Art 2 of the Basic Law for the Federal Republic of Germany [Germany], 23 May 1949.

[94] As famously framed in S Warren and L Brandeis, 'The Right to Privacy' (1890) 4(5) HLR 193.

[95] H Pearce, 'Personality, property and other provocations: exploring the conceptual muddle of data protection rights under EU law' (2018) 4(2) EDPL 190. Also see *Pfeifer v Austria* (2009) 48 EHRR 8 on reputation as part of 'personal identity and psychological integrity' protected within the right to private life.

[96] *Reklos v Greece* (2009) EMLR 16; *Peck v United Kingdom* (2003) 36 EHRR 41.

interpretations'.[97] In *Satakunnan,* the Grand Chamber of the ECtHR read a right to 'informational self-determination' within the 'right to private life'.[98] The idea of informational self-determination confers a generic right of control over one's personal information and its dissemination to other people.[99] The paradigmatic example of the breadth of this right comes from the ECtHR judgment in *Von Hannover*.[100] In this case, the Court found that Germany violated article 8 ECHR by permitting the publication in German press of photographs depicting the Princess Caroline of Monaco engaging in daily activities in public places. While the breadth in scope is not to be equated with always according greater weight to privacy over expression,[101] it allows claimants to bring forth privacy claims and seek to convince the Court for their weight in the particular circumstances.

The picture is quite different when looking at the conception of 'privacy' in UK tort law. The privacy tort has its origins in the equitable wrong of breach of confidence,[102] which required a pre-existing relationship of confidence between the claimant and the defendant. Within the law of confidence, the existence of such a relationship (eg between a doctor and her patient or a lawyer and her client) confers a 'reasonable expectation' that information disclosed between the two parties will be kept private. In *Campbell,* the House of Lords effectively established the new privacy tort, holding that a pre-existing confidential relationship is not necessary when the publisher 'knows or

[97] G Phillipson, 'Privacy: the development of breach of confidence – the clearest case of horizontal effect?' in D Hoffman (ed) *The Impact of the UK Human Rights Act on Private Law* (CUP 2011) 67.

[98] Supra n 50 at 137: 'Article 8 of the Convention thus provides for the right to a form of i*nformational self-determination*, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged' (emphasis added).

[99] S Allen, 'Remembering and Forgetting – Protecting Privacy Rights in the Digital Age' (2015) 1(3) EDPL 164, 175.

[100] *Von Hannover v Germany* (2005) 40 EHRR 1.

[101] Eg *Von Hannover v Germany (no 2)* (2012) 55 EHRR 15.

[102] Supra n 55.

ought to have known that the other person can *reasonably* expect his privacy to be protected' (emphasis added).[103]

The new cause of action was not framed as an all-embracing cause of action for invasion of privacy, but as a tort which prohibited the disclosure of *specific* information about a claimant that ought to have been kept secret. In cases following *Campbell,* the Court of Appeal further elaborated on the centrality of 'reasonable expectations of privacy' within the new tort.[104] The test of reasonable expectations is framed as an 'objective' test, which takes into consideration various factors (eg nature of the information, form, purpose and effect of the publication, absence of consent etc),[105] even if it is considered from the point of view of the right holder.[106] In practice, 'reasonableness' is not constructed in a social or cultural vacuum. Courts enquire into whether the applicant's expectations of privacy are consistent with 'societal attitudes' to the information or activity in question: would 'reasonable' people expect to be protected from exposure in a case like the one at issue?[107]

It is not difficult to observe how the requirement of 'reasonable expectations' imposes limitations for individuals seeking to bring forth a privacy claim. Without an over-arching right to informational self-determination, it is necessary to establish that there was a disclosure of information that a 'reasonable' person would want to maintain control over. In so-far case law, UK courts have interpreted this requirement as necessarily connected with a specific aspect of one's private life, disclosure of information about which would cause embarrassment and humiliation. In *Campbell,* (then) Baroness Hale found nothing 'essentially private' in Naomi Campbell 'popping out to the shops for a bottle of milk', with Lord Hoffmann concurring that only a

[103] Campbell supra n 56 at 85 (per Lord Hope).

[104] *McKennitt v Ash* [2008] QB 73 at 16 (per Buxton LJ); *JIH v News Group Newspapers Ltd* [2011] EMLR 9 at 55 (per Tugendhat J); *Thornton v TMG Ltd* [2010] EWHC 1414 at 36 (per Tugendhat J).

[105] *Murray v Express Newspapers Ltd* [2008] 3 WLR 1360 at 27 (per Sir Anthony Clarke MR).

[106] *Weller v Associated Newspapers Ltd* [2016] 1 WLR 1541 at 36 (per Lord Dyson MR).

[107] NA Moreham, 'Unpacking the reasonable expectation of privacy test' (2018) 134 Law Quarterly Review 651.

situation of 'humiliation or severe embarrassment' would justify a reasonable expectation of privacy.[108] Phillipson has argued that this conception makes it harder to establish a violation when leaving the confines of one's 'private space', where information about such sensitive aspects as health, sexuality or finance matters is usually held.[109]

This narrow reading of the scope of the privacy tort was consistently followed in subsequent High Court judgments.[110] By contrast, the ECtHR has time and again clarified that 'reasonable expectations' of privacy are certainly relevant within its assessment of an article 8 ECHR violation, yet far from conclusive. In *Pay v UK,* the Court clarified that an individual's reasonable expectations of privacy 'may be a significant, though not necessarily a conclusive factor'.[111] In the recent case of *Barbulescu v Romania,* the respondent government rose the objection that the applicant had been notified by his employer that his electronic correspondence would be monitored while on the job premises and did, thus, not have a reasonable expectation of privacy.[112] The ECtHR was not convinced about the extent to which this notification was adequate, but, crucially, stressed that *additional* factors such as the 'scope of the monitoring, the degree of the intrusion (…) (and) whether the monitoring was justified by legitimate reasons' have to be considered.[113]

---

[108] Campbell supra n 56 at 75 (per Lord Hoffmann) and 154 (per Baroness Hale); similarly in *OBG Ltd v Allan* [2007] UKHL 21 at 293 (per Lord Walker): 'Nor can anyone (whether celebrity or nonentity) complain simply of being photographed. There must be something more: either that the photographs are genuinely embarrassing (…)'.

[109] Supra n 97 at 68.

[110] *John v Associated Newspapers Ltd* [2006] EWHC 1611 where it was held that Sir Elton John had no reasonable expectation of privacy when he was photographed standing with his driver in a London street; *X v Persons Unknown* [2006] 11 WLUK 148 at 23 (per Eady J): 'the sort of information which most people would reasonably expect to be able to keep to themselves'.

[111] *Pay v United Kingdom* (2009) 48 EHRR SE2 at 24; citing *PG v United Kingdom* (2008) 46 EHRR 51 at 56–57.

[112] *Barbulescu v Romania* [2017] 9 WLUK 42 at 65-66.

[113] Ibid at 134.

In the post-exit era, beyond the privacy tort itself as a cause of action, article 8 ECHR protection will become central to RTBF litigation. By contrast to EU law, however, the Convention does not have a 'direct effect' and domestic courts consistently consider 'reasonable expectations of privacy' as a requirement for article 8 ECHR protection.[114] As a result, the informational self-determination conception of privacy deriving from the ECHR will give way to the narrower conception of privacy within the tort of misuse of private information.[115] Surely, the change will not happen overnight, considering that the common law has incrementally and by analogy expanded to cover novel claims like the RTBF.[116] Still, rather than radically expanding the UK privacy conception in the foreseeable future,[117] it is much more likely that domestic courts will develop a 'narrower' RTBF compared to the coterminous development of the right in EU law. Why is it so important, however, if the UK ends up with a 'narrower' in scope RTBF?

iii. Implications of a 'narrower' RTBF: 'responsibilising' the data subject?

There is a fundamental tension between the rationale behind the UK privacy tort and the rationale behind the RTBF, as developed in EU data protection and human rights law. With 'reasonable expectations' lying at the heart of the legal test for establishing a violation of privacy, what the data subject did or ought to have known might put her in an 'unfavourable position'.[118] It will do so by magnifying the element of individual responsibility with regard to potential privacy harms, with prior knowledge of particular aspects of an information disclosure implying a weakening or the complete absence of an expectation of privacy. This sits at odds with the idea behind establishing the RTBF

[114] Campbell supra n 56 at 21 (per Lord Nicholls): 'Essentially the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy'.

[115] Supra n 92.

[116] Supra n 86.

[117] Since to radically change the law would be 'fundamentally at odds with the distribution of powers under the British constitution', see *Regina v Secretary of State for the Environment, Transport the Regions* [2001] UKHL 23 at 76 (per Lord Hoffmann].

[118] A Chatzinikolaou, Bărbulescu v Romania and workplace privacy: is the Grand Chamber's judgment a reason to celebrate? (Strasbourg Observers 2017).

in EU data protection law, ie mitigating the risks generated by the processing of enormous quantities of personal information on the Internet regardless of the consent or knowledge of individual data subjects.[119]

In practice, this turn towards assuming that a well-informed, rational data subject can foresee the impact of an information disclosure on her private life in the mid- or long-term threatens to erode the level of protection currently afforded by the RTBF. Individual responsibility will often be constructed by reference to societal expectations about privacy. Lord Hope stressed in *Campbell* that 'contemporary standards of morals and behaviour' dictate what types of information or activity can be deemed as 'private'.[120] As Moreham explains, the 'reasonableness' of a claimant's expectations will be established if 'reasonable people' would feel that their privacy is violated by a particular disclosure or exposure.[121] In that sense, the test depends on whether privacy is '*likely* to be respected rather than on whether it should be respected' (emphasis added).[122] While, however, societal expectations in the context of eg the protection of privacy of individuals against the press may be more long-standing and clearer, social norms around the appropriate handling and disclosure of personal information on the Internet are constantly evolving and may be hard to pin down. Thus, individuals may often find themselves unable to bring forth an RTBF claim because, according to the law, they should have had expected that their information will remain in the public domain.

More specifically, risks for individuals will derive from established assumptions about the nature of particular activities or about their own capacity to foresee and consent to the disclosure of their personal information. Taking the example of surveillance, it is part of the broader social experience of living in certain parts of the

[119] M Fazlioglu, 'Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet' (2013) 3(3) IPDL 149, 150.

[120] Campbell supra n 56 at 93 (per Lord Hope).

[121] Supra n 107 at 651.

[122] N A Moreham, 'Privacy in the Common Law: A Doctrinal and Theoretical Analysis' (2005) 121 LQR 628 at 647.

UK that a significant amount of activities happening in public spaces will be recorded on CCTV.[123] From the perspective of 'reasonable expectations', the likelihood of one walking on the streets of London and having one's picture recorded and stored for crime prevention purposes is, indeed, very likely and any corresponding expectations of privacy quite weak. This explains the conflicting judgments of domestic courts and the ECtHR in *Peck v United Kingdom,* where the Strasbourg court held that the applicant's right to private life had been violated regardless of him being in a public street.[124] When a culture of surveillance and excessive data processing is normalised by resorting to the 'likelihood' of such behaviour as a benchmark for the 'reasonableness' of expectations of privacy, the scope of protection becomes quite limited.

In the case of the RTBF, this misalignment between societal expectations and actual individual perceptions of privacy becomes very acute with regard to 'voluntarily' disclosing personal information to websites or social media platforms. It is well-established within the tort of misuse of private information that whether the defendant could understand that the disclosure was 'unwelcome' is a crucial prerequisite of liability.[125] Hence, it is quite crucial if the data subject 'voluntarily' made public or communicated to a large number of recipients the information that she now seeks to have erased.[126] These requirements, however, sit at odds with the 'wilful data negligence and laziness' that often characterises the behaviour of Internet users.[127] Users often share personal information or consent to the processing of their data by a wide number of data controllers and processors, without necessarily reading properly or

[123] L Edwards, 'Switching off the Surveillance Society? Legal Regulation of CCTV in the United Kingdom' in S Nouwt, B R. de Vries and C Prins (eds), *Reasonable Expectations of Privacy?* (Asser 2005) 91.

[124] Peck supra n 96.

[125] Supra n 107 at 660.

[126] Supra n 105 at 36 (per Sir Anthony Clarke MR): 'As we see it, the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case (…) (including the absence of consent and whether it was known or could be inferred'.

[127] M Botta and K Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) 64(3) The Antitrust Bulletin 428, 432.

understanding the 'terms and conditions' of websites.[128] As work at the intersections of privacy and behavioural economics has demonstrated,[129] the 'complex life-cycle of personal data' in our data-driven economies and societies generates multiple consequences that are not and cannot be foreseen by individuals. Placing more burden on the shoulders of individual subjects, in the advent of increasing datafication and data aggregation by Internet giants, will undermine the 'practical' and 'effective' protection of the RTBF in the UK.[130]

5. Conclusion

This article has sought to interrogate claims about the implications of Brexit for the protection of digital rights in the UK, using the example of the RTBF as a right which has paradigmatically stemmed from and developed through EU law. A careful consideration of the applicable to the RTBF legal framework after Brexit has yielded the conclusion that the level of protection is not likely to be diminished in the short term, but the British RTBF will be developed as a 'narrower' in scope right in the longer term. In the absence of EU law's direct effect in the UK, the domestic conception of privacy, within the tort of misuse of private information, will increasingly underpin RTBF litigation.

A broad, informational self-determination type of privacy facilitates the establishment of an RTBF claim by individuals who have to convince courts about the appropriate balance between their rights and the expression rights of other parties. By contrast, a narrow conception of privacy, requiring intrusion into a 'specific' and sensitive aspect of the applicant's private life (eg health, sexuality or private finances) and treating her 'reasonable expectations' of privacy as a prerequisite of protection,

[128] Ibid 440.

[129] A Acquisti and J Grossklags, 'What Can Behavioral Economics Teach Us About Privacy?' in A Acquisti, S Gritzalis, C Lambrinoudakis and S di Vimercati (eds), *Digital Privacy: Theory, Technologies, and Practices* (Auerbach 2007).

[130] *Nada v Switzerland* (2013) 56 EHRR 18 at 182.

limits the extent to which individuals can bring forth RTBF claims. The gradual, yet unavoidable transition that will take place in UK law in the aftermath of Brexit will, as it has been argued here, create significant concerns for the future protection of the right. Heroic assumptions about consent and 'voluntary' disclosure of personal information on the Internet are very likely to erode protection by disarming individuals who will struggle to establish 'reasonable expectations' of privacy in the digital world.

Looking forward, and beyond the RTBF itself, the analysis offered here indicates the need to disaggregate legal disagreements about the implications of Brexit for digital rights protection. Not all legal losses stemming from the UK's exit from the EU are necessarily equally grave, nor are the implications necessarily the same in the short- and in the long-term. Since the distinctions drawn here may not be applicable to all digital rights, it is important to consider both the legal considerations and the social realities governing the exercise of particular rights. Following such an approach, legal scholars working in the area of digital rights will be able to caution against particular risks for the protection of such rights. They will also contribute to the broader debates about the impact of Brexit on fundamental rights by offering concrete and illuminating consequences of this multi-faceted and complicated transition.