Official Secrecy and the Criminalisation of Unauthorised Disclosures

Dr Oliver Butler[1]

1. Introduction

It is now over 30 years since the Official Secrets Act 1989 came into force. The most important part of that reform was its significant narrowing of s. 2, which criminalised the unauthorised disclosure of official information. The Act was presented by the Government at the time as a "great liberalising measure".[2] Although that claim has been fiercely criticised by academics, the Act certainly decriminalised a broad range of unauthorised disclosures. However, this important reform has since been progressively undermined by the proliferation of further unauthorised disclosure offences.[3] Once this is understood, it can be seen that it has not been 30 years since official secrecy laws were last "updated".[4] This has received insufficient attention in the broader literature and reflects a broader tendency to make an inappropriate distinction between official secrecy offences and other unauthorised disclosure offences. This tendency was most recently seen in the Law Commission's law reform project on the Protection of Official Data. To attempt to reform the 1989 Act without addressing this wider process of piecemeal development will result in reforms that are incomplete and insecure. They will continue to limit the availability of public interest disclosure defences, thereby undermining freedom of expression.

In September 2020, the Law Commission of England and Wales made recommendations for the reform of the Official Secrets Acts. Of particular importance was its recommendation that there be a two statutory public interest defences, one for members of the public and

---

[1] Fellow by Special Election in Law (Fixed-Term), Wadham College, University of Oxford; Research Fellow, Bonavero Institute of Human Rights. This article is based on a chapter of my PhD thesis, funded by the AHRC. I am grateful to Dr David Erdos and Dr Kirsty Hughes for their comments on drafts of the PhD chapter on which this article is based, Dr Stephanie Palmer and Professor Gavin Phillipson for their comments during my PhD viva, Professor Lionel Bently who drew my attention to relevant US materials, and the anonymous reviewers of this piece. I am also grateful to colleagues at Law Commission of England and Wales for discussions during my time as research assistant on the Data Sharing between Public Bodies project and later as an academic consultant on the Protection of Official Data project. The views in this article, and any errors or omissions, are my own.

[2] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (Oxford: Oxford University Press, 2006), p. 927.

[3] On one 2017 count, 90 new offences were passed after 1989: Law Commission, *Protection of Official Data: A Consultation Paper* (Law. Com. No. 230, 2017). annex C. The paper was published before the Digital Economy Act 2017, pt. 5 was passed, which contains further unauthorised disclosure offences.

[4] See Prime Minister's Office, The Queen's Speech 2019, 19 December 2019, 87 to 88, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853886/Queen_s_Speech_December_2019_-_background_briefing_notes.pdf> accessed 17 September 2020.

another, available as a "last resort", for public servants.[5] Although the final report recommended a future review of other unauthorised disclosure offences, it did not consider that reform to be "as pressing as in relation to [its] other recommendations", continuing to draw a distinction between official secrecy offences and "miscellaneous" unauthorised offences.[6] This article argues that to draw such a distinction is undesirable and threatens to undermine the effectiveness of reforms of the Official Secrets Acts.

At the start of the new parliamentary session on 19th December 2019, the Government announced plans for "updating the Official Secrets Acts for the 21st century", noting the Law Commission's forthcoming report and committing to "reflect on their final recommendations".[7] The UK Parliament's Intelligence and Security Committee has also recently criticised the legislation as "not fit for purpose".[8] The importance of grasping the connections between official secrecy and unauthorised disclosure offences is clear and pressing at a time when there is widespread interest in significant reform of the Official Secrets Acts.

This paper will first discuss the distinction drawn by the Law Commission between official secrecy offences and unauthorised disclosure offences in its recent law reform project. In relegating unauthorised disclosure offences to a "miscellaneous" category, connected only by a broadly common purpose at a high level of abstraction, and whose reform is less "pressing", the Law Commission missed an important opportunity to understand the broader ecosystem within which unauthorised disclosure is criminalised and the close conceptual and historical links between such offences. The paper will then explain the historic function of official secrecy offences in reinforcing centralised authority over disclosure, in particular by prohibiting unauthorised disclosures, including those purported to be in the public interest. This function expanded to secure the discipline of officials and government sub-contractors whose loyalty could not, or would not, be secured by adequate pay and career prospects.[9] As government activity has become more data-driven, contracted-out, and individualised, so have unauthorised disclosure offences proliferated: fulfilling a modern version of this historic function. The paper will then argue that the absence of public interest defences for unauthorised

---

[5] Law Commission, *Protection of Official Data: Report* (Law. Com. No. 395, 2020), [1.38]-[1.39].
[6] Law Commission, *Protection of Official Data: Report* (Law. Com. No. 395, 2020), [1.14], [6.26], ch. 6.
[7] Prime Minister's Office, The Queen's Speech 2019, 19 December 2019, 87 to 88, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853886/Queen_s_Speech_December_2019_-_background_briefing_notes.pdf> accessed 17 September 2020.
[8] Intelligence and Security Committee, *Russia* (HC 632) (21 July 2020), [117].
[9] See David Vincent, *The Culture of Secrecy: Britain 1832-1998* (Oxford: Oxford University Press, 1998).

disclosure offences raises serious art. 10 ECHR issues, which cannot be satisfactorily addressed by ad hoc reform or the interpretative obligation of the courts under s. 3 of the Human Rights Act 1998. There is a case for overarching statutory reform.

The paper distinguishes "individual-identifying" unauthorised disclosure offences, which apply to officials and government sub-contractors, from the more general data protection offences. It argues that the former are fundamentally connected to official secrecy offences, such that a rigid distinction between the two sets of offences is inappropriate. The paper then argues that this is further demonstrated by the historical development of unauthorised disclosure offences after 1989, which progressively eroded the "liberalising" reforms of the Official Secrets Act 1989. The cloak of secrecy has slipped back over a considerable amount of information concerning critical infrastructure and data-driven central and local government functions. As demonstrated by the development of unauthorised disclosure offences in the context of taxpayer confidentiality, this process started *on the very day* the 1989 Act came into force and has expanded considerably since. Reform of the Official Secrets Acts should not be conducted in isolation from the broader ecosystem of unauthorised disclosure offences.

2. *The Distinction between Official Secrecy and Unauthorised Disclosure Offences*

In February 2017, the Law Commission published its consultation paper on the protection of official data, following a referral of the topic to the Law Commission by the Cabinet Office in late 2015.[10] The consultation paper proved highly controversial and the analysis of consultation responses was subsequently subject to a lengthy policy development stage.[11] The Law Commission's final recommendations were published in its final report on 1st September 2020.

The project marks the first major review of UK official secrecy since the Official Secrets Act 1989. The Law Commission described this project as "a unique opportunity" to review the law.[12] Its final recommendations, if accepted by this, or a future, Government and

---

[10] Law Commission, *Protection of Official Data: Summary* (Law. Com. No. 230 (Summary), February 2017), [1.1].

[11] See "Law Commission Proposals on Secrecy Law Criticised" (2017) 22(2) Comms. L. 36. See also Rob Evans, Ian Cobain and Nicola Slawson, "Government Advisers Accused of 'Full Frontal Attack' on Whistleblowers", *Guardian* (12 February 2017) <https://www.theguardian.com/uk-news/2017/feb/12/uk-government-accused-full-frontal-attack-prison-whistleblowers-media-journalists> accessed 28 June 2020.

[12] Law Commission, *Protection of Official Data: Summary* (Law. Com. No. 230 (Summary), February 2017), [1.6].

passed by this, or a future, Parliament, may result in significant changes to the law on official secrecy. It is an important time to consider whether offences outside the Official Secrets Acts should be viewed as part of that same ecosystem, as such opportunities for wide-ranging, rather than ad hoc, legislative reform are rare.

The role of unauthorised disclosure offences outside the Official Secrets Act is only briefly mentioned in the broader literature on official secrecy.[13] The Law Commission itself notes the "minimal commentary on these offences".[14] Fenwick and Phillipson do refer to the existence of "around 80 statutory provisions engendering secrecy in various areas" and observe that "many other criminal sanctions for unauthorised disclosure of information exist and some of these clearly overlap" with the Official Secrets Act 1989.[15] However, they do not undertake a deeper analysis of the relationship between these offences and official secrecy. This paper builds on this earlier recognition and provides an account that shows the deeper relationship between official secrecy and unauthorised disclosure offences.

To the Law Commission's credit, it did examine "other criminal offences that protect against unauthorised disclosures of information held by government", as well as laws relating to data protection, protected public interest disclosures, exemptions under the Freedom of Information Act 2000, and the Human Rights Act 1998, to ask whether a full review of such offences was needed.[16] Criminal provisions that protect information held by Government, other than those in the Official Secrets Acts, were included in its terms of reference and the consultation paper provided an overview of the key features of, and inconsistencies between, such offences. [17] The Law Commission grouped these offences into two broad categories: "personal information disclosure offences" and "national security disclosure offences".[18] The latter category only contains a small number of offences. Noting a lack of uniformity in

[13] For a brief mention of the "two hundred or so statutory prohibitions which have accreted around government communication", see the Afterword in David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 325.
[14] Law Commission, *Protection of Official Data: A Consultation Paper* (Law. Com. No. 230, 2017), 97, fn. 1. The examples the Law Commission cite are P Richardson (ed.), *Archbold* (London: Sweet and Maxwell, 2016), ch. 25, [373]; C Zietman, "Solicitors – Watching the Detectives" (1992) 89(30) *Law Society Guardian Gazette* 17.
[15] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 47.
[16] Law Commission, *Protection of Official Data: Summary* (Law. Com. No. 230 (Summary), February 2017), [1.9], [4.4].
[17] Law Commission, *Protection of Official Data: A Consultation Paper* (Law. Com. No. 230, 2017), [4.1].
[18] Law Commission, *Protection of Official Data: A Consultation Paper* (Law. Com. No. 230, 2017), [4.3].

drafting, the Law Commission provisionally concluded that the offences were "in need of a fuller review".[19]

In their final report, the Law Commission conceded that at a "high level of generality" both the Official Secrets Act 1989 offences and other unauthorised disclosure offences share a "common purpose", namely the criminalisation of unauthorised disclosure. It also agreed that the rationale of such offences was "not exclusively the protection of personal information but also the interests of those public functions supported by effective data collection and processing". Nevertheless, it continued to emphasise the fact that many unauthorised disclosure offences criminalise the disclosure of "'personal' information relating to identifiable individuals", characterised by a "lack of uniformity across the legislative landscape", which appeared to be "irrational". Although it recommended a full review, the Law Commission distinguished this review as less "pressing" than its other recommendations.[20]

This paper supports review and reform of unauthorised disclosure offences. However, it resists the assumption that such offences are "miscellaneous"; that they potentially overlap with but are only loosely related to official secrecy. This paper seeks to show their close connection and to argue that unauthorised information disclosure offences need to be given a much more central place in discussions about reforming the law. Although they appear to protect individual privacy in officially-held individual-identifying information, they themselves perpetuate the UK's "culture of secrecy".[21] The trend to expand their scope and number threatens to undermine attempts to reform the Official Secrets Acts, including any steps towards public interest defences.

3. Freedom of Expression, Public Interest Disclosure and the UK's Culture of Secrecy

As Vincent explains, the law is only one factor that impedes free information, important not in terms of prosecutions but in the inculcation of "more general habits of deference and ignorance" among officials.[22] Vincent argues that official secrecy sought to preserve authority

[19] Law Commission, *Protection of Official Data: A Consultation Paper* (Law. Com. No. 230, 2017), [4.21], [4.58].
[20] Law Commission, *Protection of Official Data: Report* (Law. Com. No. 395, 2020), [6.1]-[6.26].
[21] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998).
[22] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), pp. 11-12.

rather than security: to control the release of information in light of a centralised notion of the public interest.[23] Secrecy is not merely created by laws but reflects a broader culture.[24]

The emergence of official secrecy in the mid to late 1800s sought to preserve discipline over disclosures. Although this was initially sought through the development of an ideal of honourable self-restraint and reserve, it later came under strain with the employment of low-paid clerks who, unlike career civil servants, did not have the same fear of dismissal.[25] As the Government was unwilling to pay enough to secure its servants' loyalty, it turned to the criminal law.[26] The early use of s. 2 of the Official Secrets Act 1911 reflected this theme.[27] During the Cold War, junior clerks and typists on temporary contracts generated much anxiety, and more recently the increased use of government contractors and industrial or professional collaborations have further complicated official secrecy.[28]

As governmental activity has become more data-driven, more contracted out, and more reliant on individualised decision-making, unauthorised disclosure offences have multiplied in the UK. At the same time, the technological landscape has altered dramatically. In 2007, Her Majesty's Revenue and Customs (HMRC) lost 25 million child benefit records on two CDs.[29] In the 1980s, it was the fax machine that facilitated leaks.[30] Now, vast quantities of data can move between servers and in the Cloud with ease. Unauthorised disclosure offences are not distinct from official secrecy, but are a modern version of it. As Lustgarten and Leigh argue "the test of secrecy is the interests served by concealment or revelation".[31] Unauthorised disclosure offences might protect personal data and privacy. However, it cannot be ignored that they reinforce centralised authority over disclosure and exclude public interest disclosures.

---

[23] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), pp. 16, 171.
[24] See Clive Ponting, *Secrecy in Britain* (Oxford: Wiley-Blackwell, 1990), p. 1.
[25] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), pp. 36, 39-40, 81.
[26] The Official Secrets Act 1889 followed the disclosure of military intelligence by a low paid draftsman in 1887. Such military dockyards were a security risk precisely because they employed many such civil servants. See David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), pp. 86-89.
[27] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 120.
[28] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), pp. 251-254.
[29] Patrick Wintour, "Lost in the Post – 25 Millions at Risk after Data Discs Go Missing", *Guardian* (21 November 2007) <https://www.theguardian.com/politics/2007/nov/21/immigrationpolicy.economy3> accessed 26 June 2020.
[30] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 263.
[31] Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Oxford University Press, 1994), p. 31.

Prohibiting public interest disclosure is not considered necessary in the law of data protection,[32] misuse of private information,[33] or confidentiality to the Crown.[34] Yet it is routinely and broadly excluded by the criminal law, across both official secrecy and unauthorised disclosure offences. This should be rigorously questioned because the possibility of publicity is a safeguard against the abuse of power.[35]

Public interest disclosures are also key to freedom of expression, as protected by art. 10 ECHR. Although the House of Lords in *R v Shayler* rejected the argument that art. 10 ECHR was violated by the absence of a public interest defence in relation to sections 1(1), 4(1) or 4(3)(a) of the Official Secrets Act 1989, it is not clear that the decision would be made in the same way today.[36] The current ECHR jurisprudence on the necessity of public interest defences for breaches of obligations of secrecy or confidentiality by officials is a narrow gate but not a closed one.

In *Shayler*, the House of Lords held that there was no violation of art. 10 ECHR. This was because an official who sought to make a public interest disclosure could make an authorised disclosure to one of a number of other officials or seek official authorisation for a public disclosure, if necessary challenging an unlawful refusal through judicial review.[37] Given the special position of security and intelligence service members and their sensitive work, and the available safeguards, such an interference with free expression was proportionate to the legitimate objective of national security.[38] It is questionable whether the Supreme Court or the European Court of Human Rights would agree today that judicial review of a refusal to authorise disclosure is sufficient in all circumstances.

---

[32] Data Protection Act 2018, ss. 170(2)(c), 171(3)(c). See also (C-131/12) *Google Spain v AEPD* EU:C:2014:317; [2014] Q.B. 1022, [106]; General Data Protection Regulation (EU) 2016/679, arts. 6(1)(f), 9(2)(g).
[33] *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 A.C. 457; *PJS v News Group Newspapers Ltd* [2016] UKSC 26; [2016] A.C. 1081.
[34] *Attorney General v Guardian Newspapers (No. 2)* [1990] 1 A.C. 109; [1988] 3 All E.R. 545.
[35] See Stephanie Palmer, "In the Interests of the State: The Government's Proposals for Reforming Section 2 of the Official Secrets Act 1911" [1988] P.L. 523, 523.
[36] *R v Shayler* [2002] UKHL 11; [2003] 1 A.C. 247. The decision has long been criticised for adopting an naïve view of whistleblowing and the effectiveness of alternative routes to disclosure: see Fenwick and Phillipson (n 2), 941-945. See also, Law Commission, *Protection of Official Data: A Consultation Paper* (Law. Com. No. 230, 2017), [9.6], [9.64]-[9.70].
[37] *R v Shayler* [2002] UKHL 11, [27]-[33].
[38] [2002] UKHL 11, [36].

In the more recent jurisprudence of the European Court of Human Rights, a violation of art. 10 ECHR may be found in circumstances where a public interest disclosure is denied for disclosures of "last resort".[39] In *Guja v Moldova*, the dismissal of a press officer for an unauthorised public interest disclosure, relating to political interference in a prosecution, was held to violate art. 10 ECHR. The European Court of Human Rights held that although a civil servant owes a strong duty of loyalty and discretion, and so should disclose "illegal conduct or wrongdoing" in the first instance to a superior or another competent body, where this was "clearly impractical" disclosure could be made to the public as a "last resort". In determining the proportionality of the interference with freedom of expression, the Court considered the public interest, the authenticity of the information, the damage to the public authority, the officer's motive, and the nature of the penalty imposed. There was no other "effective means of remedying the wrongdoing" and the public interest in disclosure outweighed the interest in confidentiality. Dismissal was a heavy sanction, with a potentially chilling effect, and disproportionate in light of the officer's good faith and motives in relation to the disclosure of genuine letters.[40] Other similar violations have been found in *Heinisch v Germany*[41] and *Burcur v Romania*,[42] the latter concerning a criminal prosecution of a member of the Romanian Intelligence Service for the public interest disclosure of unlawful telephone tapping.

Much turns on the existence of "effective means of remedying the wrongdoing" in the circumstances of a particular case, the willingness and ability of a court to scrutinise those means, and the balance of the other factors set out by the European Court of Human Rights. There is considerable potential for legal uncertainty as to whether a prosecution under a particular unauthorised disclosure offence, without the availability of a public interest defence, would be a violation of art. 10 ECHR. This might also change over time as the means of remedying wronging become more or less effective.

It might be possible for courts to read public interest defences into statutes that omit them, using section 3 of the Human Rights Act 1998, if the failure to provide one violates art.

---

[39] ECHR jurisprudence distinguishes between public interest disclosure by civil servants and journalistic public interest disclosure, even by an employee of a State broadcaster: see *Matúz v Hungary* [2014] 10 WLUK 625; [2015] I.R.L.R. 74, [33]; *Rungainis v Latvia* (Application no. 40597/08) 14 June 2018; [2018] E.C.H.R. 507.
[40] *Guja v Moldova* [2008] 2 WLUK 257; (2011) 53 E.H.R.R. 16, [70]-[96].
[41] *Heinish v Germany* [2011] 7 WLUK 618; (2014) 58 E.H.R.R. 31.
[42] *Burcur v Romania*, Case 40238/02 8 January 2013 (unreported).

10 ECHR.[43] However, an attempt to do this in relation to s. 105 of the Utilities Act 2000 to permit protected public interest disclosures was recently rejected by the Employment Appeal Tribunal in *OFGEM v Pytel*.[44] This casts doubt over the ability and willingness of the courts to provide an interpretation of legislation that protects art. 10 ECHR in all cases. This heightens the importance of statutory reform to protect art. 10 ECHR rights.

Pytel was an economic analyst at Ofgem who made disclosures concerning the public procurement of smart meters. The parties agreed that s. 105 covered the disclosure and none of its exceptions applied. Although the Employment Tribunal relied on s. 3 of the Human Rights Act 1998 to read a protected disclosures exception into s. 105, the Employment Appeal Tribunal ultimately concluded that it was not "possible" to do so. The judgment was notable for its deference to Parliament's panoramic view of in "an area in which the court is not equipped to understand the effect of a piecemeal amendment of one provision in an intricate scheme".[45] The judgment is likely to further chill hopes that s. 3 of the Human Rights Act 1998 may offer solutions to secure art. 10 ECHR in this area.

This is not to say that the Supreme Court or the Court of Appeal could not, in light of the developing Strasbourg jurisprudence discussed above and in an appropriate case, read a public interest defence or exception into legislation on the basis of the strong interpretative obligation in s. 3 of the Human Rights Act 1998.[46] That possibility, of course, remains open. Future challenges will not concern the Utilities Act 2000, which was amended following the *Pytel* litigation.[47] The case might therefore be distinguished in other statutory contexts, although it is difficult to identify an unauthorised disclosure offence which is not embedded in an intricate statutory scheme, and where the creation of a public interest defence would not carry a set of important legal and procedural consequences across criminal, employment, contract, and transparency laws. The existence of complex broader "ramifications" for a

---

[43] The possibility that s. 3 could be "used creatively" in this way is raised in Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 939. A general statutory presumption as to "the existence of a public interest defence which must be rebutted by the public authority if it wishes to restrain publication on a blanket basis" was accepted in dicta of the Court of Appeal in *R v Shayler* [2001] EWCA Crim 1977; [2001] 1 W.L.R. 2206, [72]; see also Tom Rees, "Official Secrets: Defence of Duress of Necessity" [2001] Crim. L.R. 986.

[44] *OFGEM v Pytel* UKEAT/0044/17/JOJ (10 December 2018) (unreported). The Law Commission has stated that its understanding is that the decision is pending appeal: Law Commission, *Protection of Official Data: Report* (Law. Com. No. 395, 2020), [6.24].

[45] UKEAT/0044/17/JOJ (10 December 2018) (unreported), [10], [13], [91], [96].

[46] See *Ghaidan v Godin-Mendoza* [2004] UKHL 30; [2004] 2 A.C. 557, [30], on the strength of the obligation.

[47] Utilities Act 2000 (Amendment of Section 105) Order 2020/106, art. 2(2).

compatible interpretation have limited the possibility to use s. 3 in other contexts.[48] Future attempts to rely on s. 3 might also face another difficulty, in that creating a public interest defence might be considered to cut against a "fundamental feature" of legislation intended to centralise authority over disclosure, making such an interpretation impossible.[49]

Any divergent reasoning in later Employment Appeal Tribunal or High Court cases would do little to remove the uncertainty that disadvantages whistle blowers, as the question would remain as to which analysis applies to any one of the dozens of other unauthorised disclosure offences. Whether a judgment from the Supreme Court or the Court of Appeal could remove uncertainty about the availability of interpretative solutions would also depend on the scope of its reasoning and ease with which it could be applied to other unauthorised disclosure offences. Given the potential application of such a case to a wide range of different offences and contexts, a more cautious approach may be favoured by such a court, until it has the opportunity to hear further argument in other appropriate cases.

This is clearly far from ideal. Most public interest disclosures are of course made anonymously. This is not surprising: better not to be identified at all than to have to defend oneself from criminal accusations or challenge one's employer with provisions inserted by the Public Interest Disclosure Act 1998. This does not mean that there is no important difference between a clear statutory defence and one that might be read into a statute following legal argument. The latter is likely to be accompanied by increased costs and the delay of appeals. Investigators have a duty to investigate matters pointing towards the commission of an offence and away from it.[50] Significant legal uncertainty about the existence of a public interest defence may have a material bearing on the preliminary investigation, with possible opportunities missed, especially if investigators have a misplaced confidence in the effectiveness of complaints procedures and other authorities. Cases may therefore be dropped at a much later stage than would otherwise be the case. Even if it is not the key or only consideration, some consideration of how bad the process would be in the event of discovery, and prospects of a successful defence, may influence the decision as to whether to disclose at all. With the memory of *Ponting* and *Shayler*, one might also be forgiven for trusting a jury with a clear

[48] Compare *Re S (Minors) (Care Order: Implementation of Care Plan)* [2002] UKHL 10; [2002] 2 A.C. 291, [44]; *Bellinger v Bellinger* [2003] UKHL 21; [2003] 2 A.C. 467, [37].
[49] *Ghaidan v Godin-Mendoza* [2004] UKHL 30, [33].
[50] Code of Practice to the Criminal Procedure and Investigations Act 1996, [3.5].

statutory public interest defence more than the courts, which have historically been criticised as "more executive minded than the executive" in this area.[51]

This is not at all to deny the importance of the protection of personal information and privacy. Article 8 ECHR requires respect for private life to be secured. The increase in individualised decision-making and personal services necessarily and greatly increases the amount of private and personal information held by public authorities. The purpose of this paper is to question the extent to which the proliferation of unauthorised disclosure offences, which generally lack the public interest disclosure provisions of data protection or civil laws protecting privacy, is really in the service of the protection of personal data and privacy. It concludes that, like official secrecy, it is more in the service of central authority and discipline over disclosures. To downplay this close connection is to misunderstand the development and transformation of official secrecy in the UK. A much broader understanding of the scope of official secrecy is therefore required to produce statutory reforms that adequately protect public interest disclosures and secure art. 10 ECHR rights across the activities of government.

4. Unauthorised Disclosure Offences

Criminal law is only one area of law that regulates unauthorised disclosures of individual-identifying information. The General Data Protection Regulation 2016/679 (GDPR) and Data Protection Act 2018 provide for extensive regulation of personal data in the UK.[52] The tort of misuse of private information seeks to prevent intrusive uses of private information.[53] *Marcel* confidentiality, most recently discussed in the context of the principle of legality in *R (Ingenious Media) v HMRC*, makes it a breach of confidence for public authorities to disclose information collected pursuant to their statutory powers without clear legal authority to do so.[54]

---

[51] Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (Oxford: Oxford University Press, 1990), p. 201, echoing the famous dissent of Lord Atkin in *Liversidge v Anderson* [1942] A.C. 206; [1942] 3 All E.R. 338. Smith also notes the possibility of scepticism of the courts in the face of national security interests: A.T.H. Smith, "Security Services, Leaks and the Public Interest" (2002) 61(3) C.L.J. 514, 516. *R v Ponting* [1985] 2 WLUK 98; [1985] Crim L.R. 318; *R v Shayler* [2002] UKHL 11.

[52] This continues to be the case immediately post-Brexit.

[53] See, more recently, *PJS v News Group Newspapers Ltd* [2016] UKSC 26; noted O Butler, "Confidentiality and Intrusion: Building Storm Defences Rather than Trying to Hold Back the Tide" (2016) 75(3) C.L.J. 452 (note).

[54] See *Marcel v Metropolitan Police Commissioner* [1992] Ch. 225 (C.A.); [1992] 1 All E.R. 72; *Hoechst UK Ltd v Chemiculture Ltd* [1992] 3 WLUK 286; [1993] F.S.R. 270 (Ch.); *Re Arrows (No. 4)* [1995] 2 A.C. 75 (H.L.); [1994] 3 All E.R. 814; *Hellewell v Chief Constable of Derbyshire* [1995] 1 W.L.R. 804 (Q.B.); [1995] 4 All E.R. 473; *Woolgar v Chief Constable of Sussex Police* [2000] 1 W.L.R. 25 (C.A.); [1999] 3 All E.R. 604; *R (Ingenious Media) v HMRC [2016] UKSC 54*; [2016] 1 W.L.R. 154; noted O Butler, "Confidentiality and Public Authorities: Fundamental Rights, Legality and Disclosure for Statutory Functions" (2017) 76(2) C.L.J. 253 (note).

Practising professionals, such as legal or medical practitioners, are further regulated by professional conduct bodies, often with significant consequences for unauthorised information disclosures. Employees and contractors can normally suffer other employment disciplinary or contractual consequences for unauthorised information disclosure.

Unauthorised disclosure has been criminalised in data protection law since the mid 1980s. The Data Protection Act 2018 makes it an offence knowingly or recklessly to obtain or disclose, to procure the disclosure of, or to retain, personal data without the consent of the data controller.[55] Similar unauthorised disclosure offences existed in both the Data Protection Act 1984 and Data Protection Act 1998.[56] However, these offences apply broadly to public and private bodies, do not carry similar sentencing powers to the unauthorised disclosure offences that apply to governmental activities, and are now subject to public interest defences. They are different from the unauthorised disclosure offences that apply to officials and government sub-contractors in several important respects.

The criminal law beyond the data protection offences has a particular focus on information held by officials or government sub-contractors and employees.[57] These unauthorised disclosure offences have much in common with official secrecy offences in their comparatively narrow defences, higher sentences, restrictions on disclosures under freedom of information laws, impact on employment protections for public interest disclosures, and effects in centralising state, and especially executive, control over authorised disclosures to facilitate the effective performance of public functions.

A. Narrower Defences Alongside Increasingly Generous Data Protection Defences

The data protection offences have become subject to an increasingly broad range of defences, including public interest defences. Generally, other unauthorised disclosure offences do not contain a similar set of defences. Almost all such offences lack a statutory public interest disclosure defence.[58] Unauthorised disclosure offences have therefore maintained limited

[55] Data Protection Act 2018, s. 170(1).
[56] Data Protection Act 1984, s. 15; Data Protection Act 1998, s. 55.
[57] For two key examples, covering a large proportion of official data, see Social Security Administration Act 1992, s. 123 (Department for Work and Pensions data) and Commissioners for Revenue and Customs Act 2005, s. 19 (HMRC data).
[58] Offences in the Utilities Act 2000 and Digital Economy Act 2017 are recent exceptions.

defences for officials and government sub-contractors, while defences became more generous in the data protection offences applicable across the public-private divide.

The data protection offence in the Data Protection Act 2018 is subject to a defence where the obtaining, disclosing, procuring, or retaining was necessary for the purposes of preventing or detecting crime; was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal; or in the particular circumstances was justified as being *in the public interest*.[59] It is also subject to a defence where the defendant has a *reasonable belief* that they have a legal right to obtain, disclose, procure, or retain the data; a reasonable belief that they would have had the consent of the data controller if the controller had known the circumstances; where the disclosure was for special purposes as defined by the Act and GDRP; the disclosure was with a view to the publication by a person of any journalistic, academic, artistic or literary material; or the disclosure was in the reasonable belief that in the particular circumstances it was justified as being *in the public interest*.[60] The offence in the Data Protection Act 1998 excepted obtaining, disclosing or procuring which was necessary "for the purpose of preventing or detecting crime"; was required by law; where there was a reasonable belief in the right to obtain, disclose or procure; where there was a reasonable belief that the processor would have had the consent of the data controller; or where the act was *justified in the public interest*.[61] The Data Protection Act 1984 did not contain such defences. Public interest defences available for data protection offences have become progressively more generous. Other unauthorised disclosure offences by contrast, which generally apply to officials and government sub-contractors, almost all lack equivalent public interest defences.

B. Greater Sentencing Powers than the Data Protection Offences

Unauthorised disclosure offences concerning officials and government sub-contractors generally carry the same sentencing powers as official secrecy offences. These are higher than the data protection offences, which apply to all data processors, whether public or private individuals. In general, unauthorised disclosure offences outside the Data Protection Act 2018 carry potential sentences of up to two years imprisonment and a fine.[62] It is noteworthy that

[59] Data Protection Act 2018, s. 170(2).
[60] Data Protection Act 2018, s. 170(3).
[61] Data Protection Act 1998, s. 55(2).
[62] For two examples, see Social Security Administration Act 1992, s. 123(5) and Commissioners for Revenue and Customs Act 2005, s. 19.

this is the same sentencing power as main official secrecy offences.[63] On the other hand, the maximum penalty for the unauthorised disclosure offence in the Data Protection Act 2018 is a fine, as it was under both the Data Protection Act 1998 and Data Protection Act 1984.[64] Although the Criminal Justice and Immigration Act 2008 provided for a power of the Secretary of State to amend the Data Protection Act 1998 by order to increase the maximum sentence for the data protection offence to imprisonment for up to two years, the power was never exercised and has now been repealed by the Data Protection Act 2018.[65]

C. Impact of Unauthorised Disclosure Offences on Freedom of Information

Unauthorised disclosure offences have further important consequences for the scope of freedom of information obligations, where they criminalise disclosures that would not otherwise be criminal under data protection offences. Section 44 of the Freedom of Information Act 2000 provides an absolute exception from the freedom of information disclosure obligations on public authorities for information if its disclosure is "prohibited by or under any enactment".[66] Although in many cases it is still possible to authorise what would otherwise be an unauthorised disclosure, some statutory prohibitions on disclosure cannot be authorised.[67] The Freedom of Information (Scotland) Act 2002, contains equivalent provisions.[68] Where unauthorised disclosure offences prohibit the information from being disclosed at all in those circumstances, it therefore cannot be released via a freedom of information request.

D. Impact of Unauthorised Disclosure Offences on Whistle-blowers

---

[63] Official Secrets Act 1989, s. 10.
[64] Data Protection Act 2018, s. 196(2); Data Protection Act 1984, s. 19(2); Data Protection Act 1998, s. 60(2).
[65] Criminal Justice and Immigration Act 2008, s. 77. See Rosemary Jay, *Data Protection Law and Practice* (4th edn., London: Sweet & Maxwell, 2012), [21-32] to [21-38]; see also ICO, What Price Privacy Now? H.C. 36 (2006-2007), which argued for increased sentences under data protection law to protect personal information. It was ultimately unsuccessful. The offence in the Data Protection Act 2018, s. 170 is also only subject to a fine: Data Protection Act 2018, s. 196(2).
[66] Freedom of Information Act 2000, s. 44. See ICO, 'Prohibitions on Disclosure (section 44)', [15] <https://ico.org.uk/media/for-organisations/documents/1186/section-44-prohibitions-on-disclosure.pdf> accessed 17 January 2020.
[66] See, for example, ICO Decision Notice FS50517099, which rejected the application of the s. 44 exemption to information listed in Local Government Act 1972, sch. 12A, pt. 1, because it was not prohibited in all circumstances and nothing prohibited its disclosure in the present circumstances of that case <https://ico.org.uk/media/action-weve-taken/decision-notices/2014/970282/fs_50517099.pdf> accessed 17 January 2020.
[67] See, as an example of the latter, *Barrett v Information Commissioner and the Office for National Statistics* EA/2007/0112 (23 April 2008) (unreported), in which the Information Tribunal held that the Census Act 1920, s. 8(2) did not provide any circumstances for lawful authority to disclose the relevant information in that case.
[68] See Freedom of Information (Scotland) Act 2002, s. 26.

Unauthorised disclosure offences also reduce the protections available to public interest whistle-blowers. The provisions inserted to the Employment Rights Act 1996 by the Public Interest Disclosure Act 1998 do not apply to a disclosure if the person making the disclosure commits an offence by making it.[69] Therefore, where unauthorised disclosure offences have narrower defences than the data protection offences, for example because they lack a public interest defence, the protections for workers and employees who seek to make public interest disclosures are lost.[70]

These are important protections from employment discipline for public interest disclosures. Contractual provisions are void in so far as they purport to preclude a worker from making a protected disclosure.[71] A worker has a right not to be subjected to any detriment by the worker's employer done on the ground that the worker has made a protected disclosure.[72] This is protected by a right to complain to an employment tribunal.[73] Dismissal of an employee for making a protected disclosure is an automatically unfair dismissal, for which no qualifying period of employment or upper age limit applies.[74] Criminalisation through other unauthorised disclosure offences that lack public interest defences therefore undercut these employment protections, even where no prosecution is in fact brought in respect of the disclosure in question. This might therefore be true where a prosecution is ultimately not considered to be in the public interest, and is therefore discontinued, but the employer wishes to dismiss the employee or subjects the employee to a detriment.

Criminalisation also results in greater exposure to police and other investigatory powers. This can be of particular importance for the protection of journalistic sources, who can be shielded from civil liability or employer discipline more easily than criminal investigators. It also has a wider importance in permitting the investigation or surveillance of potential or suspected whistle-blowers.[75]

E. Centralising Control over Authorised Disclosure

[69] Employment Rights Act 1996, s. 43B(3).
[70] For an example, see *OFGEM v Pytel* UKEAT/0044/17/JOJ (10 December 2018) (unreported).
[71] Employment Rights Act 1996, s. 43J.
[72] Employment Rights Act 1996, s. 47B.
[73] Employment Rights Act 1996, s. 48(1A).
[74] Employment Rights Act 1996, s. 103A. This includes a redundancy dismissal: Employment Rights Act 1996, ss. 105(6)(6A), 108(3)(ff) and 109(2)(ff).
[75] See Jacob Rowbottom, *Media Law* (Oxford: Hart, 2018), pp. 231-39.

Unauthorised disclosure offences do not prohibit disclosure in all circumstances. They do, however, act to centralise control over disclosure. This centralisation is sometimes retained by Parliament, where there are express categories of authorised disclosure, but more often given to senior officials, and therefore, in practice, to government information lawyers.

The Commissioners for Revenue and Customs Act 2005 illustrates these centralising features well. It is an important unauthorised disclosure offence, given the scale of HMRC data processing, the sensitivity of such information, and the importance of taxpayer confidentiality to tax administration. Section 18(1) imposes wide duties of confidence on HMRC officials regarding information held by HMRC in connection with one of its functions. Section 19 criminalises the disclosure of such revenue and customs information where it relates to a person whose identity is specified in the disclosure or can be deduced from it ("individual-identifying information"). The 2005 Act allows Parliament, the Revenue and Customs Commissioners, and HMRC's information lawyers to exercise considerable control over authorised disclosures, centralising control through criminalisation.

First, Parliament specifies various categories of information to which the duty of confidence does not apply. These are listed in s. 18(2). For example, these statutory authorisations include disclosures for the purpose of civil proceedings, criminal investigations or criminal proceedings relating to a matter in respect of which HMRC has functions.[76] More broadly, s. 18(1) is also subject to any other enactment permitting disclosure.[77] Some of those grounds in s. 18(2) do enable individuals or institutions to authorise disclosure. For example, they permit disclosure made in pursuance of a court order or with the consent of each person to whom the information relates.[78] More important, however, is the effect of those provisions in centralising executive control.

Other grounds in the legislation act to centralise considerable control in the hands of the Revenue and Customs Commissioners. This is not subject to the same degree of oversight as enactments by Parliament. HMRC is a non-ministerial government department. Statutory commissioners act in the place of Government ministers. This is a measure to promote the independence of tax implementation from party politics. Tax policy, on the other hand, is

[76] Commissioners for Revenue and Customs Act 2005, ss. 18(2)(c) and (d).
[77] Commissioners for Revenue and Customs Act 2005, s. 18(3).
[78] Commissioners for Revenue and Customs Act 2005, ss. 18(2)(e) and (h) respectively.

formally made by the Treasury, which is party political. Notably, s. 18(2)(a) provides that the duty of confidence does not apply to a disclosure which is made for the purpose of a function of Revenue and Customs *and* which does not contravene any restriction imposed by the Commissioners. HMRC has an extensive information disclosure guide, which takes the form of an internal manual.[79] This can be updated at will by the Commissioners, who may thereby impose restrictions on disclosure for the purposes of HMRC functions and alter the application of s. 18(2)(a). It has a significantly centralising effect in the hands of the Commissioners.

This effect is further reinforced by s. 18(2)(b), which provides that disclosures made in accordance with s. 20 are not subject to the duty of confidence. Section 20 concerns "public interest disclosure". This is very different from a public interest defence available to a defendant who has made an unauthorised disclosure. It instead provides that a disclosure made on the instructions of the Commissioners, general or specific, of a kind specified in ss. 20(2) to (7), and where the Commissioners are satisfied that it is in the public interest, is not information to which the duty of confidence applies. Detailed instructions for public interest disclosures so defined can be found in the HMRC Information Disclosure Guide.[80] Information so disclosed cannot be further disclosed without the consent of the Commissioners.[81] Breach of this duty of confidence is also an offence under s. 19(1). The effect is to centralise decision-making about public interest disclosures.

There is a defence in s. 19(3) but it is important to understand that this too is capable of having centralising effects *in practice*. It provides a defence of reasonable belief in the lawfulness of the disclosure or in the prior and lawful publication of the information to the public. HMRC has a robust team of information lawyers. Disagreement with those lawyers would greatly undermine the plausibility of a reasonable belief in the lawfulness of disclosure and therefore the practical utility of the defence. The complex and centralising character of the information disclosure guidance encourages discussions with HMRC's information lawyers, via Data Guardians and the HMRC Information Policy and Disclosure Team.[82] Disclosure in the face of HMRC legal disagreement is therefore a high risk decision, weakening the

[79] See HMRC, 'Information Disclosure Guide' (2019) <https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide> accessed 17 January 2020.
[80] See HMRC, 'Information Disclosure Guide' (2019), IDG60000 < https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg60000> accessed 17 January 2020.
[81] Commissioners for Revenue and Customs Act 2005, s. 20(9).
[82] See HMRC, 'Information Disclosure Guide' (2019), IDG10100 <https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg10100> accessed 17 January 2020.

reasonable belief defence and therefore placing more weight on the correctness of one's own legal analysis of the lawful basis for disclosure. It would not be surprising if taking such a course of action is in fact extremely rare in practice. The effect of this would be to further centralise control over information in the hands of senior HMRC officials. Reasonable belief in the lawfulness of disclosure defences are relatively common in unauthorised disclosure offences and might be expected to have similar effects where the public authority in question has a robust and well-resourced legal team.[83]

F. Official Secrecy and Unauthorised Disclosure Offences as Fundamentally Connected

Unauthorised disclosure offences and official secrecy offences are both concentrated on official and government sub-contractors. The available defences are narrower than the general data protection offences, especially in the absence of public interest defences. They both have higher sentencing powers than general data protection offences, usually a maximum sentence of two years' imprisonment. This has important implications for freedom of information, public interest disclosure employment protections, and centralising control over information disclosure to a greater extent than under the general data protection offences.

Unauthorised disclosure offences are fundamentally connected to official secrecy offences. Both official secrecy offences and unauthorised disclosure offences enhance centralised authority and discipline over disclosure decisions. Although this may offer some greater protection for personal information and individual privacy, its purpose is to enhance trust and thereby facilitate the effective performance of public functions. Information can be readily disclosed if so authorised. This means that it is inappropriate to draw a rigid distinction between official secrecy and unauthorised disclosure offences. That drawing the distinction is inappropriate can further be seen when one understands the role of unauthorised disclosure offences in eroding the "liberalising" reforms of the Official Secrets Act 1989.

5. *The History of the Erosion of the "Liberalising" Reforms of the Official Secrets Act 1989*

A. *Section 2 of the Official Secrets Act 1911*

[83] See, for example, the defences in Social Security Administration Act 1992, s. 123(4). Note that this requires "no reasonable cause to believe otherwise", which is arguably even more demanding than the reasonable belief defences in the Commissioners for Revenue and Customs Act 2005, s. 19(3).

Section 2 of the 1911 Act was incredibly broad, criminalising the unauthorised disclosure of all information obtained owing to official positions or entrusted in confidence by officials.[84] The 1911 Act was drafted to increase even further the already considerable criminal sanctions that applied to officials for unauthorised disclosure.[85] The circumstances of its passage through Parliament ensured little scrutiny. The catalyst for change was the "growing threat of international espionage" in the context of the arms race preceding the First World War.[86] This period was later described in Parliament as "the paranoia of 1911".[87] Lord Mishcon, during debates in the House of Lords on the Official Secrets Bill 1989, characterised the passage of the 1911 Act as one "passed in Parliament one afternoon in an atmosphere of some panic".[88] This context significantly strengthened the Government's hand, producing an unauthorised disclosure offence of enormous breadth. Section 2 extended to information "which [related] to or [was] used in a prohibited place", "which [had] been made or obtained in contravention" of the Act, "which [had] been entrusted in confidence… by any person holding office under His Majesty", or "which he [had] obtained owing to his position as a person who holds or has held office under His Majesty, or as a person who holds or has held a contract made on behalf of his Majesty, or as a person who is or has been employed under a person who holds or has held such an office or contract".[89]

It might be expected that the 1911 Act represented a high-water mark of such an approach in the UK. However, the 1911 Act was subsequently strengthened by both the 1920 and 1939 Official Secrets Acts. Section 1 of the Official Secrets Act 1920 broadened the provisions of the 1911 Act to include the retention of *any* official document "for any purpose prejudicial to the safety or interests of the State" when it was "contrary to his duty to retain it" or one failed "to comply with any directions issued by the Government Department or any person authorised by such department with regard to the return or disposal" of the document. It also made it an offence to permit others to have possession of official documents "issued for

---

[84] Official Secrets Act 1911, s. 2(1)(a).
[85] Official Secrets Act 1889.
[86] Michael Everett, "The Official Secrets Acts and Official Secrecy" (House of Commons Library, Briefing Paper Number CBPO7422, 17 December 2015), 6, 11.
[87] H.C. Deb. 21 December 1988, vol. 144, col. 483.
[88] H.L. Deb. 9 March 1989, vol. 504, col. 1610.
[89] Official Secrets Act 1911, s. 2(1). The 1911 Act also made it an offence to retain certain documents without a right to do so or when it was contrary to the person's duty: Official Secrets Act 1911, s. 2(1)(b). Knowing receipt or receipt with reasonable ground to believe that the material or information was communicated in contravention of the Act was an offence, unless proved that the communication was contrary to the person's desire: Official Secrets Act 1911, s. 2(2).

his use alone" or to communicate secret code words or passwords or to possess them where they had been issued to another person or, having obtained or found an official document, neglected or failed to restore it to the person or authority by whom or for whose use it was issued or to the police. The 1920 Act also introduced important evidential presumptions. It provided that communication with foreign agents *was evidence of* the commission of certain offences under the Official Secrets Acts.[90] The Official Secrets Act 1939 made further amendments relating to investigating offences under the Acts for the purpose of making prosecutions easier to obtain, by creating powers to require the furnishing of information relating to official secrecy offences.[91] This made the criminalisation of unauthorised disclosures made by officials, government employees and government contractors extremely broad.

B. *The Reform of Section 2 of the Official Secrets Act 1911 as a 'Liberalising' Reform*

Attempts to amend s. 2 of the 1911 Act had been made in Parliament as early as 1939.[92] Criticisms of excessive secrecy were made in the 1968 Fulton Report, which led to the establishment of the 1972 Franks Committee and its recommendations to reform s. 2.[93] Similar proposals were also made by the Labour Government in 1978, which led to the Conservative Government's unsuccessful Protection of Information Bill 1979.[94] A series of unsuccessful Private Members' Bills sought to reform s. 2 in the 1980s.[95] It was finally the Conservative Government, following a 1988 White Paper, that passed legislation to reform s. 2.[96]

---

[90] Official Secrets Act 1920, s. 2.
[91] Official Secrets Act 1939, s. 1.
[92] See Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (Oxford: Routledge, 1991), p. 207.
[93] Report of the Fulton Committee on the Civil Service (Cmnd. 3638, June 1968). Departmental Committee on Section 2 of the Official Secrets Act 1911 (Cmnd. 5104, September 1972). See Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), p. 208. The Conservative Manifesto in 1970 had promised to address unnecessary official secrecy: see Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), p. 189. The Labour Manifesto committed to open government in October 1974: David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 252.
[94] *Reform of Section 2 of the Official Secrets Act 1911* (White Paper, Cmnd. 7285, July 1978). See Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), p. 210. See also Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 223: Lustgarten and Leigh argue that the 1979 Bill was withdrawn due to opposition over a broad criminal provision that made the disclosure of *any* information relating to intelligence, security, or the authorised interception of communications an offence.
[95] See Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), pp. 209-211. Those Bills included the Freedom of Information Bill 1981, the Freedom of Information (No. 2) Bill 1984, and the Protection of Information Bill 1987 which contained provisions to reform s. 2 of the Official Secrets Act 1911. The last of these ultimately failed because the Conservative Government opposed it in order to pursue their own White Paper and Bill. See also Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 23.
[96] *Reform of Section 2 of the Official Secrets Act 1911* (White Paper, Cmnd. 7285, July 1978).

The reform of s. 2 of the Official Secrets Act 1911 was portrayed by the Home Secretary Douglas Hurd in 1989 as a "great liberalising measure".[97] It certainly decriminalised a broad range of potential unauthorised disclosures across wide areas of Government activity, limiting offences in the Official Secrets Act 1989 to disclosures relating to security and intelligence, defence, international relations, and crime and special investigative powers.[98] This narrowed the scope of the criminal law.[99] There was no longer a "blanket" criminalisation of unauthorised official disclosures, protecting the Government from mere embarrassment.[100] However, the claim that the Official Secrets Act 1989 was a truly "liberalising" reform has been fiercely criticised by academics.[101] That unauthorised disclosure offences have eroded even those dubiously "liberalising" reforms should be a source of significant concern, calling for close scrutiny.

Soon after the 1989 Act came into force, Ewing and Gearty argued that the reforms merely "feigned" liberalisation and were in fact "notably illiberal".[102] They argued that although the scope of the criminal law had narrowed, its scope remained broad in respect of the remaining categories. This, they argued, resulted in a broader range of information falling within the scope of the law than would have been the case had the Franks Committee recommendations been implemented. The Franks recommendations would only have covered information classified as "seriously damaging" if disclosed, in practice information classified as "top secret" or "secret".[103] The continued broad application of offences to the media also undermined its liberal credentials. With no rights to information and the broad application of offences to the media, the imprecision and uncertainty of the Act would "have a considerable

---

[97] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 927.
[98] Official Secrets Act 1989, ss. 1-6.
[99] See Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), pp. 207, 215.
[100] Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), p. 215.
[101] Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), p. 206: "Indeed it is hard to see how it can seriously or justifiably be seen as a liberalising measure at all". Stephanie Palmer, "In the Interests of the State: The Government's Proposals for Reforming Section 2 of the Official Secrets Act 1911" [1988] P.L. 523, 534: "they are far from being the 'liberalising' measures that the Home Secretary, Douglas Hurd, suggests".
[102] Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), pp. 200, 207.
[103] Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), pp. 191, 199-200.

chilling effect on freedom of expression", as would the absence of public interest and prior disclosure defences.[104]

Fenwick and Phillipson commented that, although the introduction of harm tests, mens rea requirements, and the decriminalisation of recipients are "usually viewed as liberalising features", the Official Secrets Act 1989's application to those other than Crown servants and its omissions of freedom of information provisions, public interest or prior disclosure defences, and a general requirement to prove mens rea was "arguably as significant".[105] They argued that the absence of a public interest defence, in a "statute aimed specially at those best placed to know of corruption or malpractice in government", was the fact that argued "strongly against the likelihood that [the Official Secrets Act 1989] will have a liberalising impact".[106] Amendments to add a public interest defence were rejected by the Government and defeated in both the House of Commons and the House of Lords.[107] Lustgarten and Leigh characterise the Conservative Government's approach in this period as a flat refusal to enact freedom of information legislation combined with "successive measures to lock the gates more securely with the machinery of criminal law".[108]

Fenwick and Phillipson argued that, although the "claim of liberalisation" and the impression that anomalies are resolved might give "greater government credibility" to the Official Secrets Act 1989, the complexity of its overlapping provisions could result in a greater chilling effect and therefore carry a greater deterrent effect on the press than the Official Secrets Act 1911.[109] As Thomas observes, the Official Secrets Act 1989 was a "sharper tool" to deal with leaks.[110]

---

[104] Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), pp. 199-206.
[105] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 927.
[106] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 939.
[107] Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), p. 211; see also Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), p. 203.
[108] Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 222.
[109] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 947.
[110] Rosamund Thomas, *Espionage and Secrecy: The Official Secrets Act 1911-1989 of the United Kingdom* (1991), p. 213.

Prior to its reform, the use of s. 2 had been discredited, which undermined the ability of prosecutors to secure convictions.[111] Vincent concludes that the 1989 Act "was a measure of the Conservative's entrenched reluctance to weaken the authority of the state".[112] Palmer observes that "it is tempting to conclude that the primary rationale behind this reform [was] to tighten the criminal law of secrecy, with the aim of making convictions more likely".[113] She concludes that it left "unchanged the ethos of secrecy".[114]

There had never been extensive prosecutions under s. 2.[115] In part, this is because criminalisation always played a more important role in perpetuating a "culture of secrecy" by its mere existence, rather than its frequent use.[116] From the mid 1970s, Labour had made the decision not to use s. 2, save "in the most grave circumstances".[117]

However, s. 2 became more commonly used during the years of the Thatcher Government.[118] Many of those prosecutions did not involve national security.[119] The use of s. 2 came under increased criticism. Cauldfield J's summing up and directions in *Aitken*, on trial for the disclosure of facts a Government report that could have been equally obtained from other public sources, criticised the use of the 1911 Act and called for s. 2 to be "pensioned off".[120] The imprisonment of *Tisdall* for six months for disclosing documents that revealed proposals to delay a Government announcement and so curtail the opportunity for parliamentary scrutiny further discredited the 1911 Act.[121] That this ultimately undermined the

---

[111] See Keith Ewing and Conor Gearty, *Freedom under Thatcher: Civil Liberties in Modern Britain* (1990), p. 189. Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 924; Stephanie Palmer, "Tightening Secrecy Law: The Official Secrets Act 1989" (1990) P.L. 243, 243.
[112] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 310.
[113] Stephanie Palmer, "Tightening Secrecy Law: The Official Secrets Act 1989" (1990) P.L. 243, 243.
[114] Stephanie Palmer, "Tightening Secrecy Law: The Official Secrets Act 1989" (1990) P.L. 243, 255.
[115] There were a limited number of exceptions: see David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 11, which points out there was an average of less than one prosecution every two years until 1979. See also *R v Fell* [1963] Crim. L.R. 207; 113 L.J. 580.
[116] See David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998).
[117] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 259.
[118] Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 223; see also David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), pp. 11, 262: between 1979 and 1984 there was on average one prosecution every 18 weeks.
[119] Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 223; see also David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 11: "the great majority of the cases involved relatively trivial offences".
[120] See discussion of this unreported case in Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), pp. 924-925.
[121] *R v Tisdall* (1984) 6 Cr. App. R. (S.) 155; (1984) The Times, 26 March; See Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 925; David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 264.

ability of prosecutors to secure convictions is most apparent from the outcome of the *Ponting* trial.[122] Clive Ponting disclosed documents relating to the sinking of the *Belgrano* during the Falklands war to circumvent the Secretary of State for Defence's refusal to disclose those documents in response to parliamentary questions. In the face of a judicial directions that left no defence available in law, the jury famously acquitted, effectively refusing to convict despite the clear facts and judicial direction on the applicable law.[123] Lustgarten and Leigh comment that this was "widely interpreted as rending section 2 virtually unusable".[124] Fenwick and Phillipson suggest that the *Ponting* case may have resulted in decisions not to prosecute other cases and to prefer the pursuit of civil remedies.[125] Vincent notes the advantages of "comparative speed, reliability, and lack of drama" that made civil remedies attractive to the state, as well as the absence of juries and the reduced prospect of creating "martyrs".[126] However, civil remedies were also to have their limits, as the House of Lords in the Spycatcher litigation held that the duty of confidence to the Crown, unlike official secrecy, could be outweighed by a public interest in its disclosure.[127] A.T.H. Smith suggests that it was the Conservative Government's defeats in the Ponting trial in 1985 and the Spycatcher litigation, ending in 1988, that inspired legislative reform in 1989.[128] The point was made by opponents of the Bill in Parliament, though to little effect.[129]

The 1989 Act replaced s. 2 with "provisions protecting more limited classes of official information", narrowing official secrecy but maintaining a focus on key areas of state concern.[130] It protected six categories of information: security and intelligence, defence, international relations, crime and special investigation powers, information resulting from

---

[122] *R v Ponting* [1985] 2 WLUK 98. For a detailed analysis of the case, see Rosamund Thomas, "The British Official Secrets Acts 1911 – 1939 and the Ponting Case" (1986) Crim. L.R. 491.
[123] See discussion of this in Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), pp. 925-926; Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 230; David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 265; Stephanie Palmer, "Tightening Secrecy Law: The Official Secrets Act 1989" (1990) P.L. 243, 246.
[124] Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 223.
[125] Helen Fenwick and Gavin Phillipson, *Media Freedom under the Human Rights Act* (2006), p. 926. The examples given are the decision not to prosecute Cathy Massiter for disclosures relating to alleged illegal surveillance of trade unionists and anti-nuclear weapons campaigners and the decision to bring civil proceedings against the Guardian and Observer in *Attorney General v Guardian Newspapers Ltd (No. 2)* [1990] 1 A.C. 109 ("the Spycatcher litigation"). See also Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), p. 223.
[126] David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 287.
[127] *Attorney General v Guardian Newspapers Ltd (No. 2)* [1990] 1 A.C. 109.
[128] A.T.H. Smith, "Security Services, Leaks and the Public Interest" (2002) 61(3) C.L.J. 514, 514.
[129] H.C. Deb. 21 December 1988, vol. 144, col. 489.
[130] Official Secrets Act 1989, preamble.

unauthorised disclosures or entrusted in confidence, and information entrusted in confidence to other states or international organisations.[131] The 1989 Act, while protecting the secrecy of such information, directs officials towards formal channels for authorised disclosure. Section 7 provided that authorised disclosures by Crown servants or notified persons could be "made with lawful authority if, and only if, it is made in accordance with his official duty". Such authorised disclosures could be made by government contractors "if, and only if, it [was] made in accordance with an official authorisation or for the purposes of the functions by virtue of which he is a government contractor and without contravening an official restriction". For other persons, authorised disclosures could be made "if, and only if, it is made to a Crown servant for the purposes of his functions as such or in accordance with an official authorisation". A belief, with no reasonable cause to believe otherwise, that a person had lawful authority, was also made a defence. Several attempts to introduce public interest defences to the Bill were defeated.[132] The 1989 Act did not create freedom of information rights: internal discipline would still apply to breaches and there were no positive rights to disclosure.[133]

Although the extent to which the Official Secrets Act 1989 can properly be described as "liberalising", as the Government purported it to be, it was substantially decriminalising. The Home Secretary Douglas Hurd had not hidden his criticism that the law was "*both* too wide and too weak".[134] It strengthened government control of information while decriminalising a broad range of other information. It then becomes important to ask why so many unauthorised disclosure offences were passed in the next 30 years. These were presumably understood to criminalise disclosures that were not already covered by the 1989 Act or to bring other benefits that the Act lacked. Although some do overlap, many relate to information that cannot relate to intelligence and security, defence or crime. So the current

---

[131] Official Secrets Act 1989, ss. 1-6.
[132] H.C. Deb. 22 February 1989, vol. 147, cols. 1036-50; H.L. Deb. 03 April 1989, vol. 505, cols. 906-58.
[133] Freedom of information rights were of course later created by the Freedom of Information Act 2000, which created a general right of access to information held by public authorities: Freedom of Information Act 2000, s. 1. Such disclosures are of course now authorised disclosures. However, the 2000 Act was drafted to avoid undermining the criminalisation of unauthorised disclosures offences. Information relating to national security, defence, international relations are all subject to exemptions: Freedom of Information Act 2000, ss. 24 to 27. However, these are not absolute exemptions and so are subject to a public interest test for disclosure: Freedom of Information Act 2000, s. 2. Importantly, there is an absolute exemption for information if its disclosure is "prohibited by or under any enactment": Freedom of Information Act 2000, ss. 44(1)(a) and 2(3)(h). This means that freedom of information is excluded by the existence of any unauthorised disclosure offence and no public interest test is applied. Personal data is also subject to an absolute exception if disclosure would breach data protection principles: see Freedom of Information Act 2000, s. 40.
[134] H.C. Deb. 21 December 1988, vol. 144, col. 460 (emphasis added). See David Vincent, *The Culture of Secrecy: Britain 1832-1998* (1998), p. 257.

state of the criminal law is in fact even less liberal than the dubious claims for the "liberalising" reform of 1989. This paper argues that this development has been with important implications for reform of the law in this area. It must be addressed.

C. Erosion of the "Liberalising" Reforms with Unauthorised Disclosure Offences

A very large number of other offences of unauthorised disclosure have been created by statute. The Law Commission of England and Wales recently identified 124 such offences and further offences have been passed since it published that research.[135] 90 of the unauthorised disclosure offences identified by the Law Commission were passed in or after 1989. Although the criminal law has never returned to the breadth and scope of the law as it was under s. 2, this has gradually eroded the impact of the reforms in the Official Secrets Act 1989.

This carries an important set of implications. First, we should not focus exclusively on the Official Secrets Acts when thinking about official secrecy in the UK. Perhaps under the noble guise of the protection of personal information and privacy, offences modelled on official secrets offences have proliferated. Specific offences now cover much ground that was decriminalised by the purportedly "liberalising" reforms of 1989. We should be concerned that the criminal law is even less liberal than it was in 1989. It is not enough to simply remain alert to attempts to insert unauthorised disclosure offences into legislation without public interest defences. This has been largely ineffective. There is a need for overarching reform.

Many unauthorised disclosure offences do not simply protect all information gathered pursuant to the exercise of statutory power or in the course of official duties, employment or the administration of statutory schemes. Instead, like taxpayer confidentiality, many protect individual-identifying information[136] or commercial information,[137] such as manufacturing

---

[135] Law Commission, *Protection of Official Data: Report* (Law. Com. No. 395, 2020). See, for example, the Digital Economy Act 2017, ss. 50(4), 58(4), 66(10).

[136] Rehabilitation of Offenders Act 1974, ss. 9 and 9A; Civil Aviation Act 1982, s. 23; Telecommunications Act 1984, s. 101; Electricity Act 1989, s. 89; Finance Act 1989, s. 182; Water Act 1989, s. 174; Child Support Act 1991, s. 50; Criminal Justice Act 1991, s. 91; Water Industry Act 1991, s. 206; Water Resources Act 1991, s. 204; Social Security Administration Act 1992, s. 123; National Lottery Act 1993, s. 4C; Criminal Justice and Public Order Act 1994, s. 14; Bank of England Act 1998, sch. 7; Data Protection Act 1998, s. 59; Transport Act 2000, s. 143 and schs. 9 and 10; Utilities Act 2000, s. 105; Commissioners for Revenue and Customs Act 2005, s. 19; Education Act 2005, s. 109; Childcare Act 2006, s. 13B; Companies Act 2006, s. 460; Statistics and Registration Service Act 2007, s. 39; UK Borders Act 2007, s. 42; Health and Social Care Act 2008, s. 76; Postal Services Act 2011, s. 56; Civil Aviation Act 2012, sch. 6; Welfare Reform Act 2012, s. 129; Defence Reform Act 2014, sch. 5; Mesothelioma Act 2014, s. 8; Criminal Justice and Courts Act 2015, sch. 10, paras. 15 and 25.

[137] See Coal Industry Nationalisation Act 1946, s. 56(1); Industrial Organisation and Development Act 1947, s. 5; Statistics of Trade Act 1947, s. 9; Prevention of Damage by Pests Act 1949, s. 22(5); Medicines Act 1968, s. 118;

processes, trade secrets and other information about businesses. This reflects a more targeted approach than the pre-1989 approach to official secrecy, but it often remains concerned to facilitate information processing activities for the performance of public functions. This is because such offences facilitate centralised control over official information and facilitate the collection of information for official purposes by reassuring individuals and businesses that their information cannot be disclosed without proper authorisation. Unlike the 1989 Act, these offences do not require proof of the likelihood of damage to any particular interest.

The most significant unauthorised disclosure provisions cover a vast amount of information concerning the administration of tax,[138] social security,[139] prisons,[140] youth detention accommodation,[141] and contracted out secure colleges or secure college functions.[142] Others unauthorised disclosure offences restrict the disclosure of information gathered under statutory powers to regulate a broad range activity including civil aviation,[143] telecommunications licensing and standards,[144] electricity supplier licensing and standards,[145] water supply, sewerage and rivers management,[146] railways,[147] banking,[148] data protection,[149] communications networks and services and television and radio,[150] compliance with the

---

Sea Fish Industry Act 1970, s. 14; Carriage of Goods (Prohibition of Discrimination) Regulations 1977, SI 1977/276, reg. 9(2); Highways Act 1980, s. 292(4); Fisheries Act 1981, s. 12; Public Passenger Vehicles Act 1981, s. 54; Industrial Training Act 1982, s. 6; Building Act 1984, s. 96; Telecommunications Act 1984, s. 101; Airports Act 1986, s. 74; Electricity Act 1989, s. 98; Water Act 1989, s. 174; Town and Country Planning Act 1990, ss. 196C and 325, sch. 15, para. 14; Water Industry Act 1991, s. 206; Water Resources Act 1991, s. 204; Water Resources Act 1991, s. 205; Railways Act 1993, s. 145; Goods Vehicles (Licensing of Operators) Act 1995, s. 35; Chemical Weapons Act 1996, s. 32; Airports (Groundhandling) Regulations 1997, SI 1997/2389, reg. 23; Bank of England Act 1998, sch. 7; Data Protection Act 1998, s. 59; Landmines Act 1998, s. 19; Nuclear Safeguards Act 2000, s. 6; Transport Act 2000, s. 143 and schs. 9 and 10; Utilities Act 2000, s. 105; Communications Act 2003, s. 393; Companies Act 2006, s. 460; Wireless Telegraphy Act 2006, s. 111; Cluster Munitions (Prohibitions) Act 2010, s. 23; Postal Services Act 2011, s. 56; Civil Aviation Act 2012, sch. 6; Defence Reform Act 2014, sch. 5.

[138] Finance Act 1989, s. 182; National Lottery Act 1993, s. 4C; Commissioners for Revenue and Customs Act 2005, s. 19; UK Borders Act 2007, s. 42.

[139] Finance Act 1989, s. 182; Child Support Act 1991, s. 50; Social Security Administration Act 1992, s. 123; Education Act 2005, s. 109; Childcare Act 2006, s. 13B; Welfare Reform Act 2012, s. 129.

[140] Criminal Justice Act 1991, s. 91.

[141] Criminal Justice and Public Order Act 1994, s. 14.

[142] Criminal Justice and Courts Act 2015, sch. 10.

[143] Civil Aviation Act 1982, s. 23; Airports (Groundhandling) Regulations 1997, SI 1997/2389, reg. 23.

[144] Telecommunications Act 1984, s. 101.

[145] Electricity Act 1989, s. 57: replaced by the Utilities Act 2000, s. 105.

[146] Water Act 1989, s. 182; Water Industry Act 1991, s. 206; Water Resources Act 1991, s. 204.

[147] Railways Act 1993, s. 145.

[148] Bank of England Act 1998, sch. 7.

[149] Data Protection Act 1998, s. 59.

[150] Communications Act 2003, s. 393; Wireless Telegraphy Act 2006, s. 111. These provisions covers information with respect to particular businesses.

Companies Act 2006,[151] health and social care professionals and standards,[152] postal services,[153] airports,[154] defence procurement,[155] and even the Diffuse Mesothelioma Payment Scheme.[156] Galison has argued, in the context of the US secrecy laws, that the growth in secrecy from the 1990s and in the 2000s, most notably in the Patriot Act 2001, reflected a turn to "targetable infrastructure" as the subject of US secrecy law.[157] It is difficult not to notice the similar focus on critical infrastructure in the proliferation of UK unauthorised disclosure offences after 1989.

The absence of public interest defences is significant. It is in the detail of these personal information driven, individualised decision-making heavy, oft contracted out fields that public interest disclosure is so important. We neglect that these offences are represent the modern form of official secrecy at our peril. It casts a wide net over information that may otherwise be the subject of a public interest disclosure. The cloak of secrecy has slipped over a considerable amount of information and governmental activity since 1989.

Examples of offences that exclude public interest disclosures do exist but they are very much the exception. The unauthorised disclosure offence concerning information obtained in the regulation of gas and electricity does not apply to protected disclosures under the Employment Rights Act 1996.[158] This resulted from an amendment to s. 105 of the Utilities Act 2000 made in March 2020, which removes the incompatibility with art. 10 ECHR found by the Employment Tribunal in *Pytel v OFGEM*, which was conceded by Ofgem before the Employment Appeal Tribunal.[159]

The Digital Economy Act 2017 created extensive data sharing powers for a very wide range of public authorities and utilities to disclose information to improve or target a public service provided to, or to facilitate the provision of a benefit to, individuals or households to improve their well-being; to take action in connection to debt owed to a public authority or to the Crown; to take action in connection with fraud against a public authority; or for research

[151] Companies Act 2006, s. 460.
[152] Health and Social Care Act 2008, s. 76.
[153] Postal Services Act 2011, s. 56.
[154] Civil Aviation Act 2012, sch. 6.
[155] Defence Reform Act 2014, sch. 5.
[156] Mesothelioma Act 2014, s. 8.
[157] Peter Galison, "Secrecy in Three Acts" (2010) 77 Social Research 941, 962.
[158] Utilities Act 2000, s. 105(4)(g)(ii).
[159] Utilities Act 2000 (Amendment of Section 105) Order 2020/106, art. 2(2); *OFGEM v Pytel* UKEAT/0044/17/JOJ (10 December 2018), [63].

purposes.[160] This included several personal information unauthorised disclosure offences. Three of those offences do not apply to a disclosure which consists of a protected disclosure for the purposes of the Employment Rights Act 1996 or is "publication of information for the purposes of journalism, where the publication of the information is in the public interest".[161] This was the fruit of successful lobbying by the National Union of Journalists, which resulted in a late amendment to the legislation.[162] Similar exceptions nevertheless do not apply to the unauthorised information disclosure offences in relation to information from HMRC.[163] It is unsatisfactory to rely on union lobbying and late amendment to legislation and, indeed, it is a rare case of its success in protecting art. 10 ECHR.

This also has important implications for reform of the Official Secrets Acts. This is because a flawed understanding of such offences will result in a flawed assessment of the Official Secrets Acts. Some of these offences could overlap with public interest disclosures within the scope of the official secrets offences. For example, a public interest disclosure about financial impropriety at concerning national security, defence or international relations might be made with individual-identifiable tax information.[164] A public interest disclosure about improper influence by a foreign Government in the regulation of telecommunications networks might be made with information with respect to a particular business obtained in the exercise of powers conferred by the Communications Act 2003.[165]

Reform of the Official Secrets Acts, including new public interest defences, could be easily undercut by the proliferation of unauthorised information disclosure offences. Any efforts to introduce a public interest defence for the Official Secrets Acts will therefore be vulnerable to circumvention by threatening public interest disclosers with unauthorised disclosure offences that lack any clear applicable statutory defence. Any future public interest defence for the Official Secrets Act must therefore apply widely to other unauthorised disclosure offences. Such public interest defences should be on the face of the statute, not hoped to be read into the legislation as a "last resort" to protect freedom of expression. Waiting for

---

[160] Digital Economy Act 2017, ss. 35, 48, 56, 64.
[161] Digital Economy Act 2017, ss. 41(2)(h)-(i), 50(2)(h)-(i), 58(2)(h)-(i), 66(7)(h)-(i).
[162] National Union of Journalists, "NUJ Wins Safeguards for Journalists in the Digital Economy Bill" (9 February 2017) <https://www.nuj.org.uk/news/nuj-wins-safeguards-for-journalists-in-the-digital-economy-bill/> accessed 28 June 2020.
[163] Digital Economy Act 2017, ss. 42, 51, 59, 67.
[164] Commissioners for Revenue and Customs Act 2005, s. 19.
[165] Communications Act 2003, s. 393.

the eventual amendment of provisions following art. 10 ECHR criticism in the Employment Tribunal, as precipitated the amendment of s. 105 of the Utilities Act 2000, is a wholly inadequate state of affairs.

The majority of such offences cover official information that was formerly covered by s. 2 of the Official Secrets Act 1911. They act to enhance executive control over that information. A clear example of this is taxpayer confidentiality. Below, I analyse the criminalisation of disclosures related to taxpayer confidentiality in detail. It is an important example due to the amount of information and number of officials covered by its provisions. HMRC processes a vast amount of data about individuals and its officials make up a significant proportion of civil servants in central government. This case study shows that even though offences related to taxpayer confidentiality, like many other offences, concern individual-identifying information and therefore individual privacy, the facilitation of state functions plays a major role in their potential justification.

D. Taxpayer Confidentiality as an Erosion of the "Liberalising" Reforms of 1989

For much of the 20th century, secrecy in relation to taxpayer information could be enforced through the criminal law in the Official Secrets Acts and through internal disciplinary proceedings.[166] Mba argues that, from the introduction of solemn declarations of secrecy by tax officials in the Income Tax Act 1799, "it is arguable that the primary rationale for tax secrecy was not the protection of privacy of taxpayers *per se* but the facilitation of the imposition and collection of income tax".[167] There has been consistent and long-standing recognition of the role of taxpayer confidentiality in facilitating the collection of tax.[168] Its rationale and nature shares much in common with official secrecy offences, despite its focus on individual-identifying information.

---

[166] Osita Mba, "Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality" (2012) 2 British Tax Review 187, 207.

[167] Osita Mba, "Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality" (2012) 2 British Tax Review 187, 205.

[168] See *Inland Revenue Commissioners v National Federation of Self-Employed and Small Businesses Ltd* [1982] A.C. 617 (H.L.), 633; Andrew Goodall, "Taxpayer Confidentiality: Harnett sets out HMRC View for MPs" (2011) Tax Journal <https://www.taxjournal.com/articles/taxpayer-confidentiality-harnett-sets-out-hmrc-view-mps-34761> accessed 17 January 2020; Andrew Goodall, "MPs ask HMRC to Justify Taxpayer Confidentiality", (2014) Accounting Web, <http://www.accountingweb.co.uk/tax/hmrc-policy/mps-ask-hmrc-to-justify-taxpayer-confidentiality> accessed 17 January 2020; Lord Ashton of Hyde, H..L Deb. 14 March 2016, vol. 769, col. 1580.

Taxpayer confidentiality also illustrates the way in which such unauthorised information disclosure offences are part of a wider, if ad hoc, erosion of the reform of s. 2 of the Official Secrets Act 1911. This can be seen through a more detailed historical consideration of parliamentary interventions made during the enactment of the Official Secrets Act 1989 and the policy changes which followed. In 1989, a number of MPs voiced concern that the removal of a criminal sanction for the unauthorised disclosure of taxpayer information would damage the collection of tax. Concerns for taxpayer confidentiality were also voiced in the House of Lords, as were hopes that the matter would be addressed in the Finance Bill of the same year.[169] The value of taxpayer confidentiality was once again stressed in terms of the effective operation of the tax system.[170] Chris Patten MP, the Minister for Oversees Development, announced during debates on reform of the Official Secrets Acts that separate criminal provision would be made to protect taxpayer confidentiality, although it would be targeted at information about taxpayers, including companies, and exclude information about tax policy and administration.[171] Patten also noted at that time that other areas might need further criminal legislation in the future. This would be considered on a Bill by Bill basis.[172] Lord Belstead finally confirmed in the House of Lords that the Government's intention was to make provision in the Finance Bill to protect taxpayer confidentiality through the criminal law.[173]

Section 182 of the Finance Act 1989 was introduced to protect taxpayer information following the narrowing of Official Secrets legislation in that year.[174] The section came into force on the *same day* as the repeal of s. 2.[175] Taxpayer confidentiality was therefore never without the protection of the criminal law. Unlike official secrets legislation, s. 182 and later protections have focussed on identifiable persons and not all information relating to tax. However, it would be wrong to argue that this represents only a focus on the protection of personal information and privacy. Taxpayer confidentiality was and is understood to play an important role in ensuring the effective collection of tax, an important state interest. Denying confidentiality to taxpayers was seen as threatening the tax base and it is this, rather than a concern for individual interests and values, that has driven the protection of taxpayer

[169] Lord Houghton of Sowerby, H.L. Deb. 9 March 1989, vol. 504, col. 1619.
[170] Lord Houghton of Sowerby, H.L. Deb. 9 March 1989, vol. 504, col. 1621.
[171] H.C. Deb. 22 February 1989, vol. 147, col. 1073.
[172] H.C. Deb. 22 February 1989, vol. 147, col. 1074.
[173] H.L. Deb. 09 March 1989, vol. 504, col. 1665.
[174] Osita Mba, "Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality" (2012) 2 British Tax Review 187, 208.
[175] Finance Act 1989, s. 182(12).

confidentiality in the UK. It is best understood as a targeted criminal offence designed to facilitate the state as much as to protect individual interests. This also explains its application to tax officials and not more generally to those wrongfully disclosing the same information, such as, for example, private accountants.

Section 182 was *successively amended* to extend to tax credit functions, child trust fund functions, certain social security functions and other audit and Ombudsmen functions.[176] Although an expanding scope of the offence to new functions was adopted by the state over time, the same rationale motivated it.

Offences protecting taxpayer confidentiality were further expanded to facilitate extensive data sharing on the merger of Inland Revenue and Excise and Custom to form HMRC in 2005. The O'Donnell Review was announced in July 2003 to consider the organisations responsible for tax policy and administration. The O'Donnell Review sought "a coherent approach to information" in order to use "information provided by taxpayers to develop a better understanding of customer needs so that policies and services can be best targeted", with the aim "to improve efficiency in the revenue departments".[177] The O'Donnell Review led to the Commissioners for Revenue and Customs Act 2005, the main purpose of which was to merge Inland Revenue and Excise and Customs to form HMRC.[178]

The Commissioners for Revenue and Customs Act 2005 merged Inland Revenue and Customs and Excise into HMRC. Section 17 facilitated an enormous pooling of information held by the Commissioners of Inland Revenue and the Commissioners of Customs and Excise, "their staff and anyone acting on their behalf". It provided that "information acquired by the Revenue and Customs in connection with a function may be used by them in connection with *any other function*", subject to any restrictions in statute or international agreements.[179] A

---

[176] Tax Credits Act 1999, s. 12(2)(a); Child Trust Funds Act 2004, s. 18(2)(a); Social Security Contributions (Transfer of Functions, etc.) Act 1999, sch. 6 para. 9(2)(a); Government of Wales Act 1998, sch. 12, para. 31(2); Budget Responsibility and National Audit Act 2011, sch. 5(2), paras. 14(2)(a) and 14(2)(b); Public Audit (Wales) Act 2013, sch. 4, para. 2; Public Services Ombudsman (Wales) Act 2005, sch. 6, para. 22(a), Scottish Public Services Ombudsman Act 2002 (Consequential Provisions and Modifications) Order 2004, SI 2004/1823, art. 10(b).

[177] Gus O'Donnell, "Financing Britain's Future: Review of the Revenue Departments" (2004), [1.20], [1.33]-[1.34].

[178] Commissioners for Revenue and Customs Bill, Bill 3 of 2004-05, Research Paper 04/90, 6 December 2004, 10.

[179] Commissioners for Revenue and Customs Act 2005, s. 17(2) (*emphasis added*).

significant feature of the merger was this enormous expansion of the use of information for any function of HMRC.

It is then in this context that we must see the statutory duty of confidence in s. 18 and the unauthorised disclosure offence in s. 19, discussed above. Such unauthorised disclosure offences are not conceptually distinct from official secrecy offences, one concerned with the protection of personal information and privacy and the other with centralising executive control over information to facilitate important state interests. Official secrecy offences and other wrongful disclosure offences are fundamentally connected through a common rationale in the facilitation of state interests through the strong centralising controls over information disclosure, without public interest defences. They have expanded over time and recriminalised the unauthorised disclosure of a great deal of information that fell within the scope of s. 2 of the 1911 Act. This process started *on the very day* the 1989 Act came into force.

6. Reviewing the Criminalisation of Unauthorised Disclosure Offences

Reform of the Official Secrets Act 1989 cannot be conducted in isolation from the broader field of unauthorised disclosure offences beyond the data protection offences. The criminalisation of unauthorised disclosure imposes greater control on disclosures by officials and government sub-contractors; uses narrow and restrictive defences, especially in relation to public interest defences; increases the sentencing powers of the courts, often to the same level as official secrecy offences; restricts freedom of information disclosure obligations; reduces the available protections for whistle-blowers; and centralises control, especially executive control, over authorised disclosure. Official secrecy offences are fundamentally connected to unauthorised disclosure offences, with a common set of potential justifications: the facilitation of public interests to which individual information privacy is merely incidental.

It is important to grasp this connection. Once it is grasped it can be seen that these offences have been eroding the "liberalising" reforms of the Official Secrets Act 1989 since the very day it came into force. The distinction between official secrecy offences and such unauthorised disclosure offences obscures this important relationship. It is especially important because the creation of many small, technical, criminal offences has not received extensive attention in Parliament or in wider debates. As Parliament and the public debate reform of the Official Secrets Act 1989 after 30 years, it is important to insist that we do not look at the

Official Secrets Act 1989 in isolation. Comprehensive and careful scrutiny of the justification for particular unauthorised disclosure offences is needed. Without it, reform of official secrecy will be seriously incomplete and readily undermined by the quiet proliferation of other unauthorised disclosure offences that do not permit public interest disclosures.