

WHISTLEBLOWING WITHOUT BORDERS: THE RISKS AND REWARDS OF TRANSNATIONAL WHISTLEBLOWING NETWORKS

Richard Hyde and Ashley Savage*

INTRODUCTION

The authors have previously examined the increasing prevalence and importance of cross-border disclosures by whistleblowers (Savage and Hyde 2013b; Hyde and Savage 2013; Hyde *et al* 2013; Savage and Hyde 2015). These disclosures may take a number of forms; a worker may go directly to a person in a state other than that which is the governing law of the contract; information derived from a disclosure may be passed across national boundaries by authorities in one jurisdiction to authorities in another; information may be disclosure on the internet, on a site hosted in a jurisdiction different to that inhabited by the whistleblower, and this information may be accessed by a person in a third State. The choice about whether and to whom to make a disclosure regarding a transnational issue is therefore important.

A major problem for whistleblowers faced with cross-jurisdictional concerns is the variable nature of the national protections afforded to them (Vaughn 2013 chapter 13; Wolfe *et al* 2014). Any subsequent action taken by national courts is inevitably constrained by national boundaries, particularly with regard to any remedial action. Even if the whistleblower succeeds in their claim, any court order must be enforced extra-territorially often requiring assistance from courts and enforcement agencies in the respondent's jurisdiction. This lack of uniformity increases the likelihood of a whistleblower being penalised. Whilst their employment position can be placed at risk, they may also be at risk of criminal or civil law sanctions, which paradoxically, may not apply in the legal jurisdiction in which the concern was raised.

Another problem is the ability of whistleblowers to ensure that the information disclosed is used to achieve their goal of having the concern addressed. An audience in a different jurisdiction may not react to the disclosure in the manner desired by the whistleblower, either due to different moral or legal frameworks governing the matters disclosed or the inability to understand or use the information to take action against the person whose conduct is the subject of the disclosure.

The UK legislation does not appear to have properly engaged with the rationale for protecting whistleblowers. The Public Interest Disclosure Act 1998, which takes effect as Part IVA of the Employment Rights Act 1996 provides a flexible regime in which workers can seek to obtain damages and or reinstatement if they suffer detrimental treatment or dismissal as a result of raising their concern. What it does not do is provide any form of framework for the effective handling of concerns by the recipients and, while it may have been inappropriate to include this in an employment rights protection, subsequent legislation, including Acts placing regulatory activities on a statutory footing have failed to include measures to support effective concern handling. The result of this oversight is evidenced in the disjointed and

piecemeal attempts by agencies prescribed to receive whistleblowing concerns to effectively discharge their function. If these prescribed agencies are unable to provide effective service delivery for domestic whistleblowers raising domestic whistleblowing concerns, how can we be sure that they are able to support cross-jurisdictional whistleblowing?

The UK legislation allows for significant detachment between the concern and protecting the whistleblower. It also fails to properly articulate why only UK workers are seen as proper participants in the regulatory network, where third country workers may be better placed to provide valuable information to network actors. It is clear that there are certain circumstances, such as tax evasion or avoidance using foreign bank accounts where the UK can only act upon information provided by foreign workers, yet there are no mechanisms by which the national government can act to protect the foreign whistleblower. Similarly, workers in a foreign slaughterhouse who are aware of horsemeat issues are not incentivised to disclose to UK regulators.

UK regulators cannot provide incentives for individuals in foreign jurisdictions to provide information as PIDA is aimed at post-dismissal or post-detriment protection for UK but not foreign workers. This is in contrast to the position in the US, but reflects the prevailing approaches in Ireland and New Zealand which draw a degree of influence from the UK protection.¹

Despite the aforementioned difficulties, whistleblowing concerns raised with regulators and enforcement bodies can provide the vital intelligence needed for those agencies to work effectively. Regulatory and enforcement agencies with responsibility for the oversight of organisations who operate across jurisdictional boundaries should have the capability to deal with those matters cross-border. Increased cross-border whistleblowing and increased intelligence sharing between agencies can improve efficiency (a welcome impact for countries enduring a current period of austerity). More importantly it opens the possibility for pro-active rather than re-active responses thus allowing agencies the scope to prevent disasters from happening in the first place.²

The purpose of the following discussion is first, to consider potential options to enhance the protection of cross-border whistleblowers. Second, in considering current examples of good practice, it will outline suggestions for the effective sharing of whistleblowing concerns by agencies. From the outset it is necessary to identify that the authors do not propose a simple, 'one-size fits all' approach to addressing this issue as to do so would ignore the full gamut of complexities, legal, practical and cultural.

CROSS-BORDER PROTECTION OF WHISTLEBLOWERS

Protection by the beneficiary jurisdiction

One must consider whether it would be preferable for the legal jurisdiction which benefits from the disclosure to provide legal protection. The authors argue that there are two central motivations for why a beneficiary jurisdiction might be empowered to do so.

Firstly, the state may simply want to protect its own citizens or indeed visitors to the jurisdiction.³ The state may be particularly motivated to protect against transportation safety

risks or food supply or even where security risks might lead to an increased risk of terrorism or criminal activity.⁴ In addition, the state may wish to protect the stability of its economy meaning that it has an interest in business transactions carried out on the world stage.

Second, the state may be motivated for paternal reasons, as a matter of national policy, to assist workers in developing countries (for example) where the focus in doing so may be to support efforts to stamp out corruption. Despite passage of the Bribery Act 2010 which is aimed at dealing with acts of bribery including those which might occur abroad, the UK chose to place emphasis on the activities of companies registered and or otherwise operating in the United Kingdom⁵ jurisdiction. Moreover, it did not extend PIDA to include protection for workers based outside of the jurisdiction. Whistleblowers must satisfy an employment tribunal that they have a UK employment contract before it will proceed. Where workers can show that they meet this condition they still face considerable evidential hurdles.

For example, for external disclosures (i.e. those not to an employer or his/her agents) they can make a disclosure to a prescribed person but their concern must fit within the class or description of that organisation.⁶ This is likely to be more difficult for a whistleblower working out of the jurisdiction. First their disclosure may not be within the remit of the person prescribed and, second, due to language issues or awareness of the legal principles the person may raise the concern with the wrong regulatory agency or may not disclose to a person prescribed at all. Wider public disclosures are protected by PIDA⁷ these are not without territorial restriction.⁸ Therefore an individual in the United Kingdom could raise a concern to a body based in a different jurisdiction and could be protected for doing so.⁹ Likewise, a worker outside of the United Kingdom could still raise a concern to a UK regulatory or enforcement protection if they have a UK employment contract. The tribunal would focus upon the recipient to which the disclosure was made and would ask whether the disclosure was 'reasonable in all of the circumstances.'¹⁰ In contrast, a whistleblower working outside of the UK jurisdiction with a contract of employment based in another jurisdiction will struggle to satisfy the tribunal that their claim should be heard, even where the respondent business is based in the UK.¹¹

Part of the difficulty with the UK approach is that there is a disconnection between the tribunal and any action taken by a regulator or enforcement body. PIDA is entirely reactive in the sense that it only allows a tribunal to grant remedies post-detriment or post-dismissal. In order to provide a gateway between the tribunal and the prescribed persons, a regulatory referral scheme was set up whereby individuals could tick a box on their ET1 claim form (see below). Research conducted by Public Concern at Work found that the system does not work well at present. This supports the author's own enquiries identified as an experience of sending freedom of information requests to prescribed persons (Savage and Hyde 2013a).

The United States arguably leads the way on protecting whistleblowers based outside of the jurisdiction. By providing legislation such as the Foreign Corrupt Practices Act 1977 and the False Claims Act 1863 (as amended). Both may be utilised by workers based outside the jurisdiction to obtain a financial reward for raising the concern. Brown suggests that for workers based in the UK there are considerable advantages in using the United States provisions compared with the UK PIDA (Brown *et al* 2013; Brown 2014). In terms of the

role of regulators, the provision of US legislation in this area means that a regulatory/enforcement organisation, namely the US Securities and Exchange Commission's (SEC) Enforcement Division takes a much more 'hands on' approach from the outset of the whistleblowing disclosure.¹² This is in direct contrast to the UK regulatory referral scheme which would require the HM Courts and Tribunals Service to send the tribunal judgment to a prescribed person following the outcome of a case.¹³

The longstanding problem associated with judicial action on matters based outside of the jurisdiction is enforcement. For example, the United Kingdom has long since grappled with the extra-territorial enforcement of *Norwich Pharmacal* orders.¹⁴ These orders require a party to provide the applicant with the identity of an alleged wrongdoer. Failure to comply can result in contempt of court proceedings brought under the Contempt of Court Act 1981 and a fine plus a maximum sentence of two years imprisonment. A number of internet companies with orders made against them have simply chosen not to acknowledge the jurisdiction of the court order making any further action extremely difficult (see further Savage 2013). Section 16 provides scope for action to be taken against individuals who fail to comply with monetary penalties. If based in the UK jurisdiction, the court could appoint bailiffs to seize goods and property to the value of the award. Outside of the jurisdiction enforcement requires the co-operation of courts based in the wrongdoer's domestic jurisdiction, and where necessary, the support of law enforcement agencies. Extradition may of course be possible, however, this costly and time-consuming process is dependent upon the jurisdiction who made the initial order having an extradition agreement in place with the jurisdiction in which the wrongdoer resides.¹⁵

Protection by regulators, enforcement bodies and those tasked to investigate matters of public concern

One should consider whether an official organisation tasked with the investigation of wrongdoing or malpractice should also bear the responsibility for protecting the whistleblower who provided the information.¹⁶ The current position in the UK suggests that regulators could and should do more. In 2013 the authors conducted extensive research of 48 national bodies with a regulatory function prescribed by PIDA to receive concerns and 408 local authorities. There were considerable differences in the way that regulators were handling concerns or even categorising concerns as coming from whistleblowers. The lack of a shared understanding of terminology and a baseline standard of protocols for handling concerns means that many regulators lack the capacity to share information even on a national level. The way that regulators handle concerns can have a knock-on effect on whether or not the whistleblower needs to seek legal protection. For example, if because of poor handling the regulator, enforcement or oversight body tips-off the alleged wrongdoer that the information came from a whistleblower then that individual is much more likely to suffer detriment or dismissal requiring them to seek protection using whistleblower protection laws. Careful handling, whether due to statutory base-line standards or soft law arrangements can assist the whistleblower and in many cases can help to safeguard their position. Where this is not possible one must consider whether the regulator/enforcement body themselves should effectively sanction the wrongdoer for subjecting the whistleblower

to any form of detrimental treatment. United Kingdom regulators currently lack this capacity in comparison to the Anti-Corruption Civil Rights Commission (ACRC) based in South Korea. The organisation is forbidden from revealing the identity of a whistleblower without their consent, they are able to order reinstatement of employees, can provide protection against disciplinary measures, can order the transfer of employees to another part of the organisation and can award of up to \$2million.¹⁷ Clearly, as a starting point safeguards to ensure the confidentiality of whistleblowers would be a positive step to protect whistleblowers including those potentially in a precarious position overseas. However, cross-border action by regulators is again likely to require judicial and criminal justice co-operation in the alleged wrongdoer's jurisdiction.

Protection by organisations with contractual agreements

The use of contractual agreements to protect whistleblowers provides a potentially effective private law solution to a public international law problem. Whilst breach of contract can lead to litigation and court action, the authors argue that it is likely to be most effective where the breach of contract leads to termination and therefore a loss of revenue. Many large western based co-operations outsource services to places such as India. In doing so they place a degree of reputational risk in the hands of companies based in those jurisdictions. Reputational risk can shed light on issues and potentially lead to resolutions. Moreover, where matters of concern arise, western corporations have expressed a willingness to seek to resolve issues. For example, fires in the factories of clothing manufacturers in Bangladesh led to a compensation scheme and the signing of an accord to work towards improving building safety (BBC News 2013).¹⁸ Provision of clauses in commercial contracts which include monetary penalties with the ultimate option of termination could incentivise the organisation based in another jurisdiction to treat the whistleblower with respect and to deal with the concern.¹⁹

Protections by international mechanism

A level of common protection for whistleblowers might be grounded in the decisions of the European Court of Human rights in the series of cases concerning whistleblowers. The Strasbourg decisions contain a wealth of public interest jurisprudence. In relation to whistleblowing, a series of recent cases are worthy of note: *Guja v Moldova*, *Bucur and Toma v Romania*,²⁰ *Heinisch v Germany*,²¹ *Rubins v Latvia*.²²

In *Guja*, the Court chose to adopt a whistleblowing-specific framework to conduct the proportionality analyses. It identified the following considerations:

- Whether the applicant had alternative channels for making the disclosure
- The public interest in the disclosed information
- The authenticity of the disclosed information
- The detriment to the Employer
- Whether the applicant acted in good faith

- Severity of the Sanction

The Strasbourg court has since followed the framework in *Heinisch v Germany*, *Bucur and Toma v Romania*, however, it has also sought to ‘cherry pick’ certain parts of the framework and use it alongside of other relevant jurisprudence. This was evident in the case of *Rubins v Latvia* whereby the court decided that the applicant’s case did not centrally concern an act of whistleblowing per se. Whilst the aforementioned framework provides scope for comprehensive consideration and proportionality balancing it can also lead to uncertainty where the Strasbourg court chooses to disregard certain parts of the framework and rigorously focus on others. Moreover, the Strasbourg court is not bound by judicial precedent.

There are also issues with the domestic application of the *Guja* principles. Firstly, whilst employment tribunals have obligations under the Human Rights Act 1998 to consider Convention rights and jurisprudence of the court (s.2 and s.6 respectively), s.2 does not force the court to apply the *Guja* framework or any other framework or decision of the Strasbourg court. Also, because the employment tribunal judgments are placed on a closed register, it is difficult for researchers to determine the application and effectiveness of these provisions in practice.

The authors suggest that it is necessary to consider whether there is a need for an international convention which provides protection for whistleblowers. One possibility is for the European Union to create a framework that provides protection for whistleblowers (Lewis 2011). In the United Kingdom, provided that the UK Parliament does not choose to ‘opt out’ of the legal measures adopted at EU level, the EU law will be given primacy over any conflicting UK legal provisions. This is arguably a stronger instrument to the Human Rights Act 1998 (UK). Section 2 (4) European Communities Act 1972 provides scope for judges to temporarily dis-apply or set aside law where it conflicts with the relevant EU provisions.²³ The HRA only allows for courts to make a declaration of incompatibility using s.4 HRA if they are unable to read down language to make the UK law compatible. This does not impact on the instant case before the court and therefore its potential as a safeguard may be diminished. Another option is to consider the provision of bilateral agreements between states with common borders, trade agreements and or common goals. Bilateral agreements exist to support shared criminal justice goals. The Police Co-operation Convention for South East Europe allows for the facilitation of joint working and information sharing. Ultimately, the ideal course of action would be the provision of multilateral agreements facilitated by an international organisation such as the United Nations. Multi-national agreements already exist in global aviation, administered by the International Civil Aviation Organisation, which is a UN agency.²⁴

CROSS-BORDER SHARING OF INFORMATION

Whilst protection of whistleblowers is central to encouraging disclosures, once a disclosure has been made it is necessary to ensure that the information is available to those who can take appropriate action to tackle the subject of the disclosure. The most appropriate body may be situated in a different jurisdiction than the information. The centrality of such information

sharing can be seen in, for example, article 38 of the UN Convention against Corruption. Therefore, the information must be shared across borders. Both the legal regime and the practical procedures for the transfer of information must be put in place.

Currently, this is not the case in many circumstances and the transfer of information is therefore inhibited. Information sharing, when it takes place, is often ad hoc and informal, involving personal contacts between individuals within different states. This approach to data sharing is precarious, depending on awareness of the appropriate destinations for data in order for the risks to be properly addressed and the decision-making of the recipients of the disclosure, who must make the decision to share the information.

The legal regime is often seen as inhibiting the sharing of information, with actors taking a risk averse approach to data-sharing in order not to be exposed to potential sanctions for breaching data protection and confidentiality requirements (Law Commission 2014). In many cases the legal framework is appropriate to allow the sharing of data, but if possible should be made clearer to ensure that the benefits of information sharing can be achieved, whilst of course continuing to protect individuals. Where there are formal schemes, the best practice derived from these schemes should be utilised to develop standards to support the sharing of data derived from whistleblowing disclosures and such principles must be put into practice more widely.

The legal regime

In order to share information the underlying legal regime must permit the information to be shared. In the EU the Data Protection Directive limits the sharing of information between entities. A data controller, which will include any recipient of a whistleblowing disclosure, cannot process personal data, which includes transferring the data to a third party, without complying with the data protection principles. Further, national legal systems impose restrictions on the transfer of information that is confidential.

The transfer of information must only be conducted where it is necessary. In the case of information derived from a whistleblowing disclosure this hurdle will be easily surmounted. Whether the disclosure concerns an identifiable individual or could identify the whistleblower, it will be necessary to transfer information where such a transfer can prevent or reduce a risk to third parties. This is an acknowledged ground justifying processing of personal data. However, the damage to the data subject should be considered, and data must not be processed where the damage to the data subject is disproportionate to the gain from processing the data. However, in most cases it will be proportionate to process where this will prevent harm to a third party. Similarly, confidential information can be shared when it is in the public interest to do so.

In some cases the data derived from a disclosure will not amount to personal data, as the data will concern an inanimate object. In this case the data can be shared more freely, as the data protection principles need not be complied with. Those wishing to share data across borders must therefore be careful when identifying the data that needs to be shared. Where the data can be confined to the risk, and not an identifiable individual responsible for the risk, then the Data Protection Directive will not apply. This data can then be shared.

Sharing personal data beyond the borders of the EU may present a challenge. In such cases the data controller must be satisfied that the jurisdiction to which information is shared provides the same level of protection as is provided within the EU.²⁵ This protection may be general, or guaranteed in relation to a specific case. Where the data is shared on the basis of a co-operation agreement between entities, it is therefore essential that the co-operation agreement deals with the protection of personal data shared under the agreement, and it will be necessary that all future multilateral agreements governing the sharing of information between state bodies consider the protection of that data, drawing on international principles and the increasing acknowledgement of data protection as an aspect of the right to private and family life (and indeed as a human right on its own account). Such agreements must not, however, be interpreted so rigidly as to prevent the sharing of information. The immense public good of sharing information must not be inhibited by unfounded concerns, and therefore drafting should be clear and precise, and allow sharing where necessary.

Best practice in information sharing

Drawing on the different examples of information sharing in a number of different contexts it is possible to make suggestions about best practice. A number of mechanisms exist that allow information derived from whistleblowers to be shared across borders. These systems can be either digital or analogue, but in all cases the ground rules governing the sharing of data exist before the information is received by the recipient who wishes to share. Some mechanisms utilise information systems that can transfer the information to those who may require such information -once the information is in the system it will be accessible to others with access to it. Other mechanisms are driven by proactive decisions to share information with those for whom it may be relevant.

Information disclosed regarding unsafe products can be shared through the RAPEX database set up under the General Product Safety Directive.²⁶ Regulators in all EU member states, plus Norway, Switzerland and Liechtenstein, have access to the database, and can use the information to take action against unsafe products, including withdrawing them from the shelves or recalling them from the hands of consumers. A similar database, known as RASFF, exists for food risks.²⁷ These databases automatically share information with those regulators who have access, and are therefore driven by the receiving State deciding to upload. A similar database is the Thetis database set up under the Paris Memorandum of Understanding, which contains details, amongst other things, of ships requiring Port-State controls. Once a ship identified on the database enters territorial waters then action can be taken.

An alternative is a system driven by the state that requires information in order to take action. The state could search a database in order to discover whether there is any information regarding the action that it wishes to take. An example of this sort of database, which is drawn from the criminal justice field, and which does not contain data derived from whistleblowers, is the system created by the Prum Decision of the EU Council,²⁸ which allows certain EU member states to inquire whether other states hold biometric data (particularly fingerprints and DNA profiles) matching those found at crime scenes. The problem with such databases holding data derived from whistleblowing is that searches tend

to be reactive, and therefore such mechanisms for data-sharing are ill suited to preventing risks arising prior to the risk eventuating, which is often the goal of whistleblowers.

Sharing information on a one-off basis is the alternative mechanism for sharing information across borders. The information is provided to the person seen as best placed to respond to the risk disclosed in the information. The recipient is determined by the person in possession of the information. This person may have difficulty identifying the most appropriate person, particularly in another jurisdiction, where the State may operate in a different way, and the division of responsibility between different levels of government and different parts of the executive may be unfamiliar and confusing. This may lead to information not being shared, or information being shared with a person who is unable to take action to address the concern. This problem could be lessened by the imposition of a legal duty to transfer information to an appropriate person. Such a legal duty is imposed ²⁹

Whether the information is shared using a system existing prior to the sharing or whether it is shared ad hoc, a number of best practices should be followed. In particular, there is a need for a shared language to be agreed. This does not necessarily mean that the information shared should be shared in one language, but that there must be a common understanding of the content of information to be shared and the terminology to be used. In previous studies it is clear that terminology means different things to different regulators at a national level (Savage and Hyde 2013a), this problem is likely to be increased and exacerbated at an international level. Therefore, agreements between regulators should carefully define the content, terms and format of information to be shared.

One problem with an information systems approach are the start-up costs necessary to create such systems. Whilst the costs are seen as worthwhile when it is anticipated that large amounts of data will be shared through the system, in cases where there are only small amounts of data shared it may be better to share on an ad hoc basis.³⁰ Therefore, systems should be used by the maximum number of states in order that the benefits are shared. This strengthens the case for a multilateral approach. Further, the information systems must be usable by all those who might wish to invoke it. File formats, metadata and hardware should be taken into account, and systems designed to be widely accessible by entities in different states.

The best system is one where there is an appropriate level of automation in the transfer, but which provides an opportunity for decisions regarding more or less extensive sharing to take place where this is necessary either to ensure that the concerns raised are addressed or that the whistleblower is properly protected. It is also necessary to ensure that there is sufficient commonality between the data shared between different states to ensure that the data shared can be used to support action.

CONCLUSION

Cross-border cases present particular problems for protecting whistleblowers. In an increasingly networked globalised market place there is an identifiable need for cross-border arrangements for whistleblowers. Whilst there are some positive indications (for example, in the US) that a whistleblower could raise concerns to another legal jurisdiction and receive a

monetary reward for doing so, this situation is atypical.³¹ The United Kingdom currently lacks the legal and regulatory framework to encourage and facilitate cross-border whistleblowing. The authors have presented some possible options for legislators to consider options for protecting cross-border whistleblowers. These suggestions all require an agreed solution to a common problem. In order for any of the aforementioned suggestions to work, effective cross-border co-operation and agreement is required at all levels from the organisations, the regulators and enforcers, to the judiciary and legislature. These suggestions do not offer simple solutions yet this complexity should not overshadow the benefit associated with facilitating and protecting cross-border whistleblowing to those who are tasked to effect action.

Bibliography

BBC News (2013), 'Rana Plaza collapse: Primark extends payments to victims' 24th October 2013, available at <<http://www.bbc.co.uk/news/business-24646942>> (accessed 15/07/15)

Howard Brown (2013), 'Corruption Cases will be the Cause of Jurisdictional Clashes' Law Society Gazette, 10th September 2013 available at <<http://www.lawgazette.co.uk/law/corruption-cases-will-be-the-cause-of-jurisdictional-clashes/5037516.article>> (accessed /14/05/15).

Howard Brown, Rose. T. Luzon, Chiharu Sekino (2014), *US Whistleblower Programmes: An Invaluable Tool to Fight against Fraud and Corruption* available at <<http://www.howard-brown-solicitor-advocate.com/#!download-the-whistleblowing-e-book/ct37>> (accessed 14/6/15)

David Huey (2014), 'The US War on Drugs and its Impact in Latin America' The Guardian, 3rd February 2014: available at <<http://www.theguardian.com/global-development-professionals-network/2014/feb/03/us-war-on-drugs-impact-in-latin-american>> (accessed 14/07/15)

Richard Hyde and Ashley Savage (2013), 'Cross-border concerns: the disclosure and sharing of information with regulators based outside the United Kingdom' International Whistleblowing Research Network Conference 2013, Middlesex University

Richard Hyde and Ashley Savage (2015), 'The Halfway House is Only Halfway Built: Towards a Fit-for-Purpose Understanding of 'Prescribed Persons' in the Public Interest Disclosure Act' SLSA Annual Conference 2015, Warwick

Richard Hyde, Ashley Savage, Bansil Desai and Jamie Grace (2013), 'Response to the Law Commission Consultation on Data Sharing between Public Bodies'

Law Commission (2014), *Data Sharing between Public Bodies* (No 351)

David Lewis (2011) 'Evidence to the European Parliament Budgetary Control Committee hearing on Whistleblowing' available at <<http://www.europarl.europa.eu/document/activities/cont/201105/20110518ATT19546/20110518ATT19546EN.pdf>> (accessed 28/6/2015)

Hugh Pennington (2009), *The public inquiry into the September 2005 outbreak of E coli O157 in South Wales* (Welsh Assembly Government)

Thomas Powell (2015), 'NHS Whistleblowing Procedures in England' SN06490, 23rd February 2015 available at <<http://researchbriefings.files.parliament.uk/documents/SN06490/SN06490.pdf>> (accessed 15/07/15).

Doug Rae (2005), *Independent Advisor to the Minister of Public Safety on outstanding questions with respect to the bombing of Air India Flight 182: Lessons to be Learned* available at <<http://www.publicsafety.gc.ca/cnt/rsracs/pblctns/lssns-lrnd/index-eng.aspx>> (accessed 14/07/15).

Ashley Savage (2013), 'The Extra-territorial Application of Norwich Pharmacal Orders' Northumbria Research Conference

Ashley Savage and Richard Hyde (2013a), 'Local Authority Handling of Freedom of Information Requests: Lessons from a research project' 19(2) Web Journal of Current Legal Issues

Ashley Savage and Richard Hyde (2013b), 'Cross-border concerns: Perils and possibilities' 2(3) E-Journal of International and Comparative Labour Studies
<http://adapt.it/EJCLS/index.php/ejcls_adapt/article/view/132>

Ashley Savage and Richard Hyde (2015), 'The response to whistleblowing by regulators: a practical perspective' 35(3) *Legal Studies* 408

Robert. G. Vaughn(2013) *The Successes and Failures of Whistleblower Laws* (Edward Elgar, Cheltenham)

Simon Wolfe, Mark Worth, Suelette Drayfus, A.J. Brown (2014), *Whistleblower Protection Laws in G20 Countries: Priorities for Action* (Blueprint for Free Speech)
<<https://blueprintforfreespeech.net/394-2/463-2>> (accessed, 14/07/15)

* Assistant Professor in Law, University of Nottingham and Senior Lecturer in Law, Northumbria University. The authors would like to express thanks to the conveners for organising an excellent and highly informative conference and to the participants for comments on the presentation.

¹ Protected Disclosures Act 2000 (NZ) Protected Disclosures Act 2014 (IRE).

² By allowing regulatory, enforcement and oversight bodies to respond to minor concerns before they become major scandals subject to a public inquiry. This was highlighted by the public inquiry into the Tudor's meat scandal (Pennington 2009)

³ This form of handling problems 'up stream' is well established. For example, in Latin America, the United States has provided financial support and training to police and armed forces personnel with the ultimate aim of reducing the flow of drugs into the United States since the 1970s (Huey 2014).

⁴ Terrorist incidents caused by a bomb which exploded on board Air India flight 182 and a bomb which went off in a Narita Airport Japan after failures in baggage checks in an Vancouver Canada Airport (together with failings of the intelligence agency CSIS) prompted a change in global policy on security checks. See further, Rae 2005.

⁵ See the relatively restrictive definition of "commercial organisation" in s. 7(5) Bribery Act 2010. Moreover, according to s.12 (4) of the Act, offences of bribing foreign officials are limited to those committed by British Citizens, and individuals "ordinarily resident in the United Kingdom." See also link to HM government website providing information for organisations: <https://www.gov.uk/government/publications/bribery-act-2010-guidance> (accessed 14/07/2015).

⁶ Section 43F Public Interest Disclosure Act 1998.

⁷ Disclosures to the wrong regulator may result in the whistleblower being unable to obtain protection. For an example of this see *Dudin v Sailsbury District Council* (2003) ET 31022631/03. It was further suggested in *Re A Company* [1983] 2 All ER 36 that disclosures of information to a regulator without the jurisdiction to look into the matters complained of would not be protected by the common law public interest defence in breach of confidence cases. See further Hyde and Savage 2015.

⁸ Following the repeal of s.196 Employment Rights Act by the Employment Rights Act 1999.

⁹ Provided that the individual can convince an Employment Tribunal that they have a UK employment contract.

¹⁰ For a full list of evidential requirements, see further s.43F Public Interest Disclosure Act 1998.

¹¹ See further: *Foxley v GPT Special Project Management Ltd* (2011) (22008793/2011). For further consideration of jurisdictional matters see: *Clyde & Co LLP and another v Bates van Winkelhof* [2013] EWCA Civ 1207 [75]-[84].

¹² However, in lieu of this neither provisions provide express pre-detriment or pre-dismissal protection codified in the legislation.

¹³ The whistleblower could of course choose to contact a regulator in the mean-time but there may be tactical implications with regards to any financial settlement. The Civil Procedure rules (1998) (UK) (governing how courts and tribunals and advocates conduct cases) specifically require parties to attempt settlement, see in particular CPR R.26 and R.36.

¹⁴ *Norwich Pharmacal Co & Others v Customs & Excise Commissioners* [1974] AC 133.

¹⁵ Whilst extradition is notably easier in the European Union due to the usage of European arrest warrants and the extensive co-operation and co-ordination between Europol and Eurojust outside of the EU, the system is reliant upon extradition treaties. The UK Crown Prosecution Service provide a list of countries:

http://www.cps.gov.uk/legal/d_to_g/extradition/annex_c_-_extradition_with_territories_outside_the_european_union/

(accessed 14/07/15). The wrongdoer can, of course, move outside of the jurisdiction in question to one where there is no agreement in place thus frustrating the process further.

¹⁶ Whilst it is acknowledged that the focus of the authors' research is based on the work of national regulators and local authorities performing a regulatory function, it is appreciated that other jurisdictions may use alternative terminology for these organisations. The authors' primary focus in this section is to consider the role of official recipient organisations whose day to day activities are focussed upon maintaining oversight and accountability of public and private organisations.

¹⁷ Act on Anti-Corruption and the Foundation of the Anti-Corruption & Civil Rights (South Korea) and ACRC webpages: <http://www.acrc.go.kr/eng/board.do?command=searchDetail&method=searchList&menuId=020312> (accessed 15/07/15).

¹⁸ See further Primark website: <http://www.primark.com/en/our-ethics/news/rana-plaza> (accessed 15/07/15).

¹⁹ It is notable also that the United Kingdom is moving towards more contractual recognition of whistleblowers (in the contracts of employment of NHS staff). See further Powell 2015.

²⁰ (2013) (Application no. 40238/02).

²¹ (2011) (Application no. 28274/08).

²² (2015) (Application no. 79040/12).

²³ The EU Charter for Fundamental Rights further enhances protection. However, because of the operation of the closed employment tribunal register it is not clear how this is being applied in whistleblowing cases at present.

²⁴ See further, organisation website: <http://www.icao.int/Pages/default.aspx> (accessed 14/07/15).

²⁵ Data Protection Directive article 25(1).

²⁶ Directive 2001/95 on general product safety, articles 11 – 13 and annex II. The database contains information about unsafe products derived from a number of sources, but it can include information derived from whistleblowing disclosures.

²⁷ Regulation 178/2002

²⁸ Decision 2008/615/JHA.

²⁹ For example, see Commission for Children and Young People Act 2012 (Victoria) section 61

³⁰ As an example, the sharing of data about aircraft safety between the UK and Tanzania was seen to be ad hoc Savage and Hyde 2013b. Whilst the sharing between UK and Tanzania might be at a small scale, a multi-national system may be both efficient and useful.

³¹ The authors are not advocating monetary rewards for whistleblowers but rather the need to support cross-border whistleblowers. To consider monetary rewards would be beyond the aims and scope of this paper.