Turning a good newsroom bad:
White collar crime, tort and case management issues arising from the UK phone hacking scandal

Judge Gibson, President, Judiciary Working Group[1],
Union Internationale des Avocats 55th Congress
1 November, 2011 - Miami

"Wrongdoers turned a good newsroom bad and this was not fully understood or adequately pursued."

James Murdoch, 7 July 2011[2].

"A mighty, wealthy family-run organization that can effectively buy up politicians and police officers: we feel we have a word for that, and it originates in Sicily rather than Sydney."

Jonathan Freedland, "10 days that shook Britain", *The Guardian,* 16 July 2011.

"Do our media brethren really want to invite Congress and prosecutors to regulate how journalists gather the news?"

Editorial, *Wall Street Journal,* 19 July 2011

Introduction

Phone tapping, computer hacking and other illegal means of information gathering can intrude into the privacy of every person who has ever used a telephone or computer. Although the information illegally obtained may be sold for large sums, ruin rival businesses or reputations, or be used to commit crimes, criminal penalties have been derisory, particularly where the information gathered has related to the private life of persons in the news[3].This discussion paper looks at how a lack of

[1] This draft discussion paper (31 July 2011) is circulated for comment and corrections prior to the Judiciary Working Group session at the UIA Miami congress. An updated and amended copy of the paper, which reviews legal issues arising from the use (or abuse) of news-gathering technology and the "phone hacking scandal", will be provided at the Congress.

[2] http://www.guardian.co.uk/media/2011/jul/07/news-of-the-world .

[3]Schedule 1 provides information about the criminal background of one agency in particular, Southern Investigations, as well as details of the sums paid to investigators. The Information Commissioner notes in "What Price Privacy" May 10, 2006 at 1.12 (see also Annexure A) that prosecutions bring minimal fines or conditional discharges, and that between November 2002 and January 2006, only two fines of more than £5,000 (and no gaol terms) were imposed. The Commissioner also noted that other investigations led to "frustrating outcomes, despite the detriment caused to individuals generally". Yet documents seized from only one detective agency, in Operation Motorman, identified 305 journalists involved in many thousands of illegal requests for data. Although this report reached over 30 million people, the follow-up report ("What Price Privacy Now", December 2006) noted the response of media commentators that journalists should be treated "differently". Judges appear to have taken a similar view on at least one occasion: Judge Paul Darlow, in a 2006 case where over 100 charges were brought concerning 93 individuals (one of whom later turned out to be Gordon Brown), expressed the view that the costs of the prosecution were disproportionate to the wrongdoing: http://www.thisisdevon.co.uk/Westcountry-detective-alleged-illegal-police/story-12933841-detail/story.html . As to civil claims, see *Malone v Metropolitan Police Commissioner* [1979] Ch 344 at 376, where Megarry V-C held no duty of confidence attached to information acquired by phone tapping, a view Sir John Donaldson, in *Francome v Mirror Group* [1984] 1 WLR 892 at 895 (an early phone tapping case) called "somewhat surprising", and which Meagher, Gummow & Lehane ("Equity:

understanding of the ramifications of misuse of modern technology led to a culture of acceptance of criminal conduct on a major scale in the United Kingdom. Corporate governance failed, not only for the media organisations whose private investigators helped them make large profits out of the illegally obtained information, but also for the Press Complaints Commission[4], political bodies and the police who failed to investigate or put a stop to this conduct until the public outcry became too great.

The legal issues for discussion, which I have reduced to three questions, relate to how the law should balance privacy with public interest where modern technology makes illegal information-gathering too easy.

For the benefit of UIA delegates from countries where there has been limited coverage of the "phone hacking scandal", I have first set out a history of "phone hacking" and complaints of media intrusion into private lives, including some of the early decisions on privacy-related issues. It starts with the *Guardian*'s crusade against phone hacking and other newsgathering methods it considered warranted investigation.

How the *Guardian* broke the phone hacking story

From 2002[5] until 2011, the *News of the World* ("*NOW*") phone hacking scandal was a lone crusade[6] by the *Guardian* newspaper, which published a series of articles complaining about unacceptable and illegal methods used by tabloid journalists gathering information, including phone hacking, payments to police and hiring private investigators of dubious repute. Phone hacking, the most common of these practices, had long been used to obtain information about celebrities; as far back as 1981, the Prince of Wales and fiancée Lady Diana Spencer had sought an injunction to restrain publication of a transcript of their telephone conversations while the Prince was in Australia; this was reported in *The Times* on 7 May 1981. When announcing their

---

Doctrines and Remedies", 1992 edition, [4109]) consider wrongly decided. See "Computer Misuse" [1999] NZLCR 54.

[4] http://www.independent.co.uk/news/media/press/we-failed-on-phone-hacking-admits-chair-of-press-watchdog-2203840.html . The PCC withdrew its 2009 report, acknowledging the results were "invalid": http://www.propublica.org/article/a-u.s.-view-of-the-phone-hacking-scandal-beware-of-press-commissions/single - note this article calls the PCC report "one of the most embarrassing reports in the history of modern journalism". However, this was only one of a series of PCC reports taking a dismissive view of telephone interception, including its 2000 report on Thurlbeck, its 2 July 2003 report concerning the *Sun* eavesdropping, its rejection of the Yorkshire Ripper's objection to his private telephone calls from prison being posted on the *NOW* website, its 2006 investigation of Mulcaire (http://www.pressgazette.co.uk/story.asp?sectioncode=1&storycode=37416) and its opposition to increased penalties under the Data Protection Act: (http://www.pressgazette.co.uk/story.asp?storycode=37683).

[5] The *Guardian* first began writing about phone hacking in 2002, warning that phone hacking was widely used to obtain information about celebrities (Celebrity "phone hacking" on the increase", 14 October 2002). The first *Guardian* article referring to investigations carried out for the media by private investigator Jonathan Rees including phone hacking was published on 21 September 2002: http://www.guardian.co.uk/uk/2002/sep/21/privacy. This information was obtained by police executing an authorized telephone surveillance on Rees' phone in the course of their investigation into the murder of Rees' partner, Daniel Morgan.

[6] The PCC and police both rejected the *Guardian*'s claims; the PCC stated that journalistic practices had "improved" after the Mulcaire prosecution: http://www.independent.co.uk/news/media/press/guardian-loses-pcc-phonehacking-case-1817261.html .

engagement, which they had kept secret for three weeks, Prince Charles actually joked he was told the phones were "tapped"[7].

In the United Kingdom, as in most countries, telephone tapping, interception and mail-opening are activities which require the issuing of a warrant to a law enforcement agency, generally the police. Such warrants are applied for where necessary, but the number is small; for example, the total number of warrants issued in 2007 for England and Wales was 1,881[8]. It is instructive to compare the annual figures for warrants issued to police with the much larger figures for phone hacking available from the records seized from private investigators, because this tells us that non-police hacking has been far greater in scale.

The *Guardian's* 14 October 2002 article warned celebrities to be careful, and noted comments to this effect by members of public relations firms:

> "According to one well known PR man, some journalists are even tapping into phones to sabotage their rivals' chances in story bidding wars by deleting messages.
>
> Hacking into strangers' mobile phone voicemail boxes is a relatively simple process but can only be used if the mobile phone user has not personalised his or her voicemail access code.
>
> "There is a certain element in Fleet Street that sees this as a new form of investigative journalism and it's getting worse," said James Herring of Taylor Herring Communications, whose clients include Richard Madeley and Judy Finnigan, Neil Morrissey and Caroline Feraday.
>
> "We always advise our clients to change the default pin number on their mobile phones straight away as this bars strangers from accessing their voicemail.
>
> "But now not only are celebrities being targeted, as journalists trawl for stories, but so are the people negotiating bids for stories.
>
> "Newspapers are accessing people's voicemails and deleting the messages left by their rivals.
>
> "This started as a dirty tricks ploy by the red-top Sunday papers but voicemail espionage has become epidemic."

The *Guardian* goes on to note PR consultant Max Clifford's assistant agrees, saying that it is "common practice" and that "everyone does it" although it is "underhand" (Max Clifford was, it would later transpire, one of the victims of the phone hacking scandal).

Another method of obtaining information the subject of the *Guardian's* campaign was police leaking information, especially if there was any allegation of payments made. Charges against police officers for supplying information to journalists were dismissed in 2000 (Neville Thurlbeck of *NOW* and DC Richard Farmer were both acquitted) and 2002 (DCI Gordon Mutch was acquitted of a charge in a case that "had important implications for the relationship between journalists and police" according to the *Guardian* report of 30 January 2002).

---

[7] http://www.youtube.com/watch?v=wg_fib2gQaU&feature=related .

[8] Figures for the number of warrants issued in England, Wales and Scotland going back to 1937 are set out by Statewatch at http://www.statewatch.org/uk-tel-tap-reports.htm .

Other persons concerned by tabloid publishers' tactics, apart from the *Guardian,* were academics, but their research related more to stalking and surreptitious photography[9] than to phone hacking. Opponents of phone hacking were ridiculed publicly by journalists such as Paul Dacre, editor of the *Daily Mail*[10] and politicians such as Boris Johnson[11]. Celebrities who complained to police or sought injunctions were often successful, but the newspapers published regardless[12].

Another problem area, the *Guardian* claimed, was chequebook journalism; problems occurred during several trials as a result of payments made to witnesses, and in one case the trial judge referred conduct of the tabloid in question the Attorney-General, but without result.[13] It seemed there was no stopping the inexhaustible flow of scandal stories about the lives of celebrities or of anyone considered newsworthy.

On 13 November 2005, *NOW* published an article about Prince William containing private information, which led to a report being made to police[14]. Prince William's security could have been compromised, and the logical question was whether this had happened to others[15]. The journalist, Clive Goodman, and the private investigator, Glen Mulcaire were duly convicted. However, police refused to consider any further investigation[16], despite having in their possession Mulcaire's notebook with over

---

[9] For example, Robin D Barnes, "Outrageous Invasions – Celebrities' Private Lives, Media and the Law", Oxford University Press, 2008 .

[10]As recently as 19 July, the day Rupert and James Murdoch were giving evidence before the UK Parliamentary committee inquiring into phone hacking, *The Times* was quoting Paul Dacre as saying that phone hacking and "blagging" could be justified in revealing "wrongdoing" and that he had sympathy for journalists who used "questionable methods" to expose matters of public interest ("Dacre backs hacking", p.3). None of the cases where hacking was used exposed wrongdoing . One of the cases where "blagging" was used, the Victoria Beckham kidnap case, resulted in the trial judge referring the conduct of the journalists to the Attorney-General ("Chequebook journalism in the dock", BBC, 3 June 2003).

[11]http://www.guardian.co.uk/media/2010/sep/15/boris-johnson-news-of-the-world-phone-hacking-codswallop

[12] See the application by Prince Charles and Lady Diana Spencer, reported in *The Times* on 7 and 9 May 1981. Despite the application being granted, the publication still appeared. Robin D Barnes (ibid, at xviii) refers to a "vast array" of law suits and (in Chapter 5 - 8), noting that successful celebrity court actions such as Princess Caroline's 10-year saga have been treated disdainfully by the press.

[13] "Chequebook journalism in the dock", BBC, 3 June 2003. Roy Greenslade (*Guardian,* 31 January 2011) notes calls for an inquiry into this practice, which resulted in the collapse of several trials.

[14] http://www.dailymail.co.uk/news/article-399814/Moment-Prince-William-discovered-voicemail-scam.html .

[15] The *Daily Mail* (*ibid*) refers to the Prince's chief of staff, a former SAS officer, expressing the concern that if this was happening to the Prince, "who on earth else could it be happening to?".

[16] The police knew in 2006 that other *NOW* journalists such as Ian Edmondson had also used Mr Mulcaire's phone hacking services: http://www.independent.co.uk/news/uk/crime/phone-hacking-now-met-police-are-in-the-dock-2178127.html. Nor was there any investigation of payments to police for information, despite Rebekah Brook's statement to an HoC Committee in 2003 that police were paid, a statement that caused considerable publicity at the time: http://www.telegraph.co.uk/news/uknews/1424573/Paying-the-police-newspapers-have-a-lot-of-form.html . This article also refers to private investigator Jonathan Rees (the subject of the chronology in Schedule 1) as obtaining information about the Royal family and the Jill Dando murder. As to the police obligation to investigate, see *Bryant & Ors, R v The Commissioner of Police of the Metropolis* [2011] EWHC 1314 (Admin), 23 May 2011, helpfully summarized at http://ukhumanrightsblog.com/2011/05/25/police-may-have-duty-to-inform-victims-of-phone-hacking/ .

12,000 references to phone numbers.[17] This was about well in excess of the number of legal wiretaps not only for England, Wales and Scotland but also the whole of the United States in one year[18].

This was also despite a widely publicised prosecution, in 2002, relating to one of the biggest phone hacking scandals in the United States, when police raided the office of Anthony "PR to the Stars" Pellicano. US police seized "11 computers, including five Macs, 23 external hard drives, a Palm V digital assistant, 52 diskettes, 34 Zip drives, 92 CD-Roms, and two DVDs," according to *Vanity Fair*[19]. This equipment contained "3.868 terabytes of data," the New York Times reported, "the equivalent of two billion pages of double-spaced text."[20] Those charged with Pellicano included not only police officers but several of his bigger clients, such as the Hollywood director John McTiernan ("Die Hard", "The Hunt for Red October", "Predator") and a well-known Hollywood lawyer. When Pellicano was arrested he had enough explosives in his office to bring down an airliner, although his target appears to have been more modest, namely the journalist at the *Los Angeles Times* (Anita Busch) who was researching him. In the course of two trials (for which he was convicted) stories of demanding money for articles not appearing in the paper, the failure of police to contact all victims and the failure to prosecute many of the other participants were reported over the period 2002 - 2010 without comment, even by the *Guardian*[21].

The change of public opinion in the United Kingdom relates to the discovery that these victims were not only celebrities but ordinary members of the public who found themselves in the public limelight not in pursuit of publicity, but after some dreadful tragedy. This included grieving relatives of murder and terrorism victims, and in particular the hacking of a mobile phone of a teenage murder victim, Milly Dowler. The relatives of Milly Dowler and police continued to believe that Milly was alive because messages on her mobile phone were being deleted[22]. Milly had been murdered prior to these message deletions; they were deleted by a private investigator retained by *NOW,* so that he could access any new messages left on her phone.

The discovery that hacking had also happened to the victims of the London 7/7 bombing and the families of soldiers killed on duty created a public outcry. The response went from denial, or saying "get over it"[23], to public apologies, but it was too little and too late. Advertisers, responding to the level of public anger, began withdrawing their advertisements from *NOW*; politicians called for inquiries; the police began making more arrests. On 7 July 2011 James Murdoch made the announcement containing the quotation I have set out at the beginning of this discussion paper, that following publication of the next issue, the newspaper would be closed down.

---

[17] http://www.mirror.co.uk/news/top-stories/2011/07/11/phone-hacking-scandal-twelve-face-prison-three-are-police-115875-23263764/ .

[18] see the US figures for wiretap warrants on p. 17.

[19] http://www.vanityfair.com/culture/features/2006/06/pellicano200606 .

[20] 11 February 2006.

[21] See for example http://www.guardian.co.uk/film/2008/dec/16/pellicano-hollywood-trial?INTCMP=SRCH . Once again, academics expressed concerns, such as Professor John S Coffee of Columbia University: "Investigator to the Stars Convicted", *NY Times* issue dated 16 May, 2008.

[22] http://www.guardian.co.uk/uk/2011/jul/04/milly-dowler-voicemail-hacked-news-of-world .

[23] This was the response of journalist Paul McMullan, who was himself the subject of hacking when his conversation was taped by actor Hugh Grant (*New Statesman*, 12 April, 2011).

When *NOW* published its last issue on 10 July 2011, it was still the most widely read English newspaper not only in England (where it enjoyed 42% of the market, according to Sir Paul Stephenson's evidence on 19 July 2011) but in the world, as well as being one of the most profitable. Its demise was not due to merger, financial mismanagement, or any of the usual reasons for business failure; it failed because of widespread public outcry at illegal business practices falling under the umbrella of "white collar crime".[24]

James Murdoch, announcing the closure, acknowledged as much when he said that the newspaper had to shut down because "wrongdoers turned a good newsroom bad"[25]. In other words, the "wrong" or "bad" conduct of company personnel (and a rolling boycott by its advertisers in response) meant that this financially successful newspaper had become so unviable it had to be shut down immediately.

The real vice in phone hacking was, as Chris Bryant MP explained to parliament, that *NOW* journalists' use of illegal means of doing business led to the creation of "dangerously close"[26] relationships with the police and persons of influence such as politicians, firstly to protect their information-gathering procedures, and then to protect the profits from their business. The same illegal means of information-gathering were then used to spy on these persons, on one occasion at the request of a notorious criminal wanting information about the police officer in charge of a murder inquest in which the criminal was the chief suspect[27].

This conduct, which the *Guardian,* in the quote at the commencement of this discussion paper, describes as originating "in Sicily", is familiar to white collar crime academics. Studies of widespread criminal activity in business affairs have looked at whether a particular industry (such as the motor trade) encourages practices which are "criminogenic"[28]. A level of "wrong" or "bad" activity in the company, coupled with denials of wrongdoing which were now known to be false, has led to a total loss of public trust and thus the failure of the business, as well as to resignations by top police officers. It would be a startling proposition to suggest, however, that journalism is a "criminogenic" trade or profession. The answer must then be found elsewhere.

---

[24] The term "white collar crime" was first coined in 1939 by E H Sutherland to describe a trusted person of high respectability who committed a crime in the course of his occupation. Traditionally, white collar crime has involved financial misappropriation or other damage to the corporation, rather than conduct that is good for company business: see "Trusted Criminals: White Collar Crime in Contemporary Society", 2009 (4th ed.), David O Friedrichs, p.2.

[25] http://www.newsoftheworld.co.uk/notw/public/nol_public_news/1347103/News-International-today-announces-that-this-Sunday-10-July-2011-will-be-the-last-issue-of-the-News-of-the-World.html (accessed 7 July 2011; many *NOW* articles are no longer available from the web).

[26] http://www.independent.co.uk/news/uk/politics/murdoch-ally-warned-mp-not-to-pursue-hacking-scandal-2238673.html .

[27] June 2002; see the entry in Schedule 1.

[28] R Apel and R Paternoster, "Understanding "criminogenic" corporate culture", in S S Simpson & D Weisburd (eds), "The Criminology of White Collar Crime", Springer, 2009, at p. 15 refer to the paradox of "why good people do dirty work", a concept echoed by James Murdoch's reference to wrongdoers turning a "good" newsroom "bad". Some academics claim the corporate structure is inherently criminogenic because of the diffusion of responsibility and prioritization of the profit motive; others claim specific organisations and industries (such as car dealers, or occupations involving technical knowledge) are particularly vulnerable; see the discussion of these theories by Hazel Croall, "Understanding White Collar Crime", Open University, Cardiff, 2007.

The questions to ask

In my opinion, these are:

- Why has the use of illegal or "wrong" newsgathering methods become so widespread by English journalists? Is this a "white collar crime" problem, or something else?

- Damage to victims has ranged from minor (personal distress) to major (loss of career and health problems). What kinds of actions and remedies should the victims have?

- What kind of matters should the inquiries looking into these events pay particular attention to?

The fallout from the phone hacking scandal raises questions that are of interest to tort, corporate and white collar crime lawyers, for the following reasons:

(a) The peremptory closure of a financially successful business because of the wrongdoing of its employees is an undesirable phenomenon requiring close examination. Did corporate governance or management problems lead to this result? Is it possible that the problem is not simply stupidity (or cupidity) but a failure to understand the ramifications of new technology, where issues concerning right and wrong conduct may not appear clear?[29] Many of the police answers to questions set out in the 20 July full parliamentary report on phone hacking (see for example those set out at [54] – [56][30]) make it clear the police considered the phone hacking to be as complex as a major fraud case, rather than a straightforward matter of proving that telephone messages were intercepted without permission.

How adequate is criminal legislation and policing when dealing with criminal cases where the evidence may be thousands of documents on a computer? Could the police refusal to investigate, and the complaint about being required to re-investigate this matter (rather than what they regarded as "real" crime)[31] be the result of lack of computer and technical skills and a misunderstanding of the law, or is this a smokescreen[32]?

---

[29] Mulcaire's lawyer told the sentencing judge that seeing others phone hacking was one of the reasons why his client did not think this conduct was illegal; Goodman's lawyer told the sentencing judge that "ethical lines are not always as clearly defined or at least observed" for journalists: http://www.ndtv.com/article/world/how-prince-william-harry-phones-were-hacked-by-tabloid-48943 . For a recent article on the ethical boundaries thrown up by electronic communication (especially the "social media" such as Facebook) see http://heinonline.org/HOL/Page?handle=hein.journals/pace31&div=9&collection=journals&set_as_cursor=7&men_tab=srchresults&terms=wire|tapping&type=matchall#230 .

[30] http://www.guardian.co.uk/media/interactive/2011/jul/20/phone-hacking-news-corporation .

[31] Many commentators have noted the police reluctance to investigate, such as the *Economist* ("Not going quietly" 27 January 2011, which noted that hacking into phones to get a juicy story had been regarded up to that time as "no big deal")

[32] The *Economist, ibid,* notes: "One defence offered by the police is that what exactly constitutes unlawful hacking is unclear. Some experts reckon the law on intercepts would not make listening to

(b) What kind of cause of action, if any, does the victim of this loss of privacy have? Is the resultant action a claim in tort, breach of confidence, damages under data protection laws, or all three? What kind of remedies are appropriate? Where the loss of privacy occurs as a result of a criminal act, is it appropriate to refer the claims to a criminal compensation scheme, rather than costs-burdened proceedings for civil damages?

(c) What are some potentially helpful lines of inquiry for the investigators into these activities? Do white collar crime theory or principles of corporate governance offer any assistance to help investigators find out what went wrong, and ensure this kind of widespread criminality does not recur?

First, the conduct in question, whether it is legal or illegal, must be examined, to determine the nature and extent of the "wrong" and "bad" conduct identified by James Murdoch which led to the newspaper's demise. Whether wrong or bad conduct is in fact the sole reason for the newspaper's shutdown on 2 days' notice may be debatable, but what is clear beyond dispute is that the nature and extent of the conduct referred to by James Murdoch as "wrong" and "bad" would have to be "endemic"[33] to warrant such an extreme step. How can a corporation be so compromised by the conduct of its employees that it has no choice but to shut down?

Some definitions of "phone hacking" and other illegal news-gathering methods

Although the word phone hacking ("wiretapping" in the United States) is generally used, this has become an "umbrella" term for a wide variety of newsgathering practices. Some of that conduct, such as bribing police officers or stealing documents, is obviously criminal in nature. The same applies to such information if it is obtained electronically. In general terms, any kind of electronic eavesdropping is a crime in most countries if the perpetrator surreptitiously gains access, through another person's telephone/computer system, to that person's confidential information in the form of emails, phone messages, SMS and internet searches.

Hacking a phone is a straightforward process and has been possible since the telephone came into existence. Hacking methods prior to modern technology are explained by Patrick Fitzgerald and Mark Leopold in "Stranger on the Line: The Secret History of Phone Tapping"[34]. A description of how it is currently done is set out in the full parliamentary report on phone hacking[35].

---

someone's messages after that person had heard them an offence, distasteful as it might seem. Mark Stephens of Finers Stephens Innocent, a media law firm, says that "the law on telephone intercepts predates mobile-phone technology and that created a grey area."" This claim has no support in case law (see *DPP v Fordham* [2010] NSWSC 958 at [27] where the sentencing judge described as "astounding" evidence from a media lawyer that the *Listening Devices Act* 1984 (NSW) was "of some complexity"). Nor is there basis in fact; Fitzgerald and Leopold ("Stranger on the Line: the Secret History of Phonetapping", London, 1987, at pp. 234 – 6) presciently pointed out in 1987, the same telephone tapping methods can be used for both.

[33]This was the word used in a question put to Mr Rupert Murdoch during the parliamentary session on 19 July 2011.

[34] The Bodley Head, London, 1987, at pp. 196 – 221.

[35] *Loc. cit*., at [98] et seq.

Are there different kinds of phone hacking?

While phone hacking is, in the absence of authorization, illegal, how it is treated depends upon whether the phone hacking is done for commercial gain, criminal purposes or other motives. Phone hacking and electronic eavesdropping tend to fall into one or more of the following categories:

1. "Hacktivism" – first used in 2005 by Jason Sack[36] to describe breaking into sites for a political rather than financial motive, such as defacing or redirecting websites. An example is the Anonymous collective attack on Church of Scientology.

2. Amateur hacking – this is a relatively old phenomenon going back to ham radio operators. Early claims that amateurs were responsible for the "Squidgygate" tapes have now been discounted. Amateur hacking is performed out of interest in the technology or "purely for fun"[37], not financial motives.

3. Hacking for profit – journalists obtaining stories, businesses obtaining insider information or spying on rivals. This is not just tortious wrongdoing, but a crime.

4. Hacking into telephones or similar activities by organised crime.

5. Cyber warfare[38] and intelligence activities, which have been on the increase since 9/11 and the "war on terror".

Eavesdropping has always been against the law. In 1769 Blackstone stated that at common law:

> "Eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behaviour."[39]

Early cases on phone hacking and tapping

In 1981, Simon Regan, a former journalist from *News of the World*, obtained transcripts of telephone calls made by Prince Charles from Australia to Lady Diana Spencer, his fiancée. It says much for the innocence of those times that the most exciting things said were Prince Charles' disparaging remarks about the Australian Prime Minister, Malcolm Fraser. Prince Charles and Lady Diana obtained an

---

[36] See his *InfoNation* article about Shu Lea Cheang.
[37] Fitzgerald & Leopold, *loc. cit.,* at p. 224.
[38] The history of security-related phone tapping in the United Kingdom (up until 1987) can be found in Fitzgerald & Leopold, *ibid.* For a study of cyber warfare in the United States as at 2004, see http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf .
[39] 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, 169 (1769). This quotation was obtained from the CRS Report for congress, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdroppping", updated September 2, 2008, by Gina Stevens and Charles Doyle.

injunction (The Times, 7 May 1981[40]) but the German magazine *Die Aktuelle* bought the transcripts and published them despite a German court also holding that these documents should not be published as not only were the conversations private but they were obtained through an unauthorized wiretap (The Times, 9 May, 1981).

In 1993 Australia again became the centre of attention when one of the most notorious taped conversations, the 1989 conversation between Prince Charles and his mistress, was published by *New Idea*, a women's magazine owned by a corporation which formed part of News International[41].

There are other ways of obtaining information, such as paying a former employee to reveal confidential details of their employment. This conduct is not illegal, although the employee may be in breach of contractual obligations. In 1983 the Queen obtained orders restraining publication of private details by a former Palace employee.[42] However, the increasing media practice of ascribing information and quotations to unnamed "friends" or "insiders" has become an alternative to payments to former employees, and such statements may possibly be based on information gleaned from telephone intercepts; if so, it is material which is illegally obtained. A variant on this form of conduct occurs where the former employee/girlfriend and/or the journalist offers not to publish if paid money[43]. This method was extensively used by Anthony Pellicano, as his Wikipedia entry notes[44]. This method may also involve the use of technology where the "friend" or "insider" is in fact material obtained by phone hacking. Similarly, "blagging", the practice of obtaining banking or other confidential information by false representations, is often done by reliance upon information obtained by phone hacking[45].

Although the Royal Family enjoyed some early success in court, they were defeated by the flexibility of electronic publication. Members of the Royal Family were subject to a series of illegal recordings, such as the "Squidgygate" Princess Diana tapes (untruthfully claimed to have been made by ham radio operators[46]), telephoto

---

[40] "Prince Charles given injunction on telephone tapping", *The Times*, 7 May 1981, p. 1; Patricia Clough and Frances Gibb, "German weekly prints its version of royal conversations", *The Times*, 9 May 1981, p. 1.

[41] http://www.smh.com.au/world/camillagate-scoop-raises-questions-for-murdoch-20110730-1i5cf.html

[42] http://www.time.com/time/magazine/article/0,9171,953753-1,00.html . For an interesting recent article about misuse of material by employees, see "Peeping" 24 BERKTLJ 1167, which makes recommendations for computer programme designers to prevent the increasing misuse of computer-generated information.

[43] http://thebsreport.wordpress.com/2009/09/23/john-travolta-victim-of-29-5-million-blackmail-plot/ is a US example where an attempt to obtain money from a celebrity resulted in charges being laid.

[44] http://en.wikipedia.org/wiki/Anthony_Pellicano .

[45] "Blagging' is where an unauthorised person obtains personal information—addresses, telephone numbers, medical information, financial information, etc—from a source that legitimately hold the information by pretending to be either the individual whose information is held or someone else with a legitimate right to access the information."
http://www.guardian.co.uk/media/interactive/2011/jul/20/phone-hacking-news-corporation , Chapter 2, footnote 15.

[46] http://en.wikipedia.org/wiki/Squidgygate .

lens photos and scams involving fake Sheiks[47], paparazzi and "stalkerazzi" pursuit which over the past thirty years has been extended to many celebrities[48].

The Empire Strikes Back

In 2004 the European Court of Human Rights handed down judgment in the decade of appeals in *Case of von Hannover v Germany* (2004) 40 ECHR 1[49]. This judgment should have discouraged some of the excesses of the tabloid press but like other judgments handed down in the previous thirty years, it made little difference.

The facts were as follows. The plaintiff, Princess Caroline of Monaco, lived in Monaco, and under French law enjoyed a degree of protection from tabloid excesses. However, German tabloids published articles about her continually, and many were less than flattering. In 1993 she sought an injunction in the Hamburg Regional Court (Langericht) against any further publication in Germany by the Burda publishing group. She directed her complaint to a series of 43 photographs of her with her children with such unflattering captions as "her life is a novel with countless disasters" and "Princess Caroline fell flat on her face". Her claim was that these photos infringed her right to protection of her personality and private life as guaranteed by Articles 2-1 and 1-1 of the Basic Law and Article 22 et seq of the Copyright Act. The case was appealed all the way to the European Court of Human Rights.

The Court, in interpreting the Convention as a whole, noted that Article 10 provided for free expression, but that there was a difference between reporting facts contributing to public debate in a democracy about matters such as government and political matters and details of the private life of someone who exercises no official function. Zupančič J went on to note:

> "I adhere to the hesitations raised by my colleague, Judge Cabral Barreto. And while I find the distinctions between the different levels of permitted exposure, as defined by the German legal system, too *Begriffsjurisprudenz*-like, I nevertheless believe that the balancing test between the public's right to know on the one hand and the affected person's right to privacy on the other hand must be adequately performed. He who willingly steps onto the public stage cannot claim to be a private person entitled to anonymity. Royalty, actors, academics, politicians, etc. perform whatever they perform publicly. They may not seek publicity, yet, by definition, their image is to some extent public property.
>
> Here I intend to concentrate not so much on the public's right to know – this applies first and foremost to the issue of the freedom of the press and the constitutional doctrine concerning it – but rather on the simple fact that it is impossible to separate by an iron curtain private life from public performance. The absolute *incognito* existence is the privilege of Robinson; the rest of us all attract to a greater or smaller degree the interest of other people.

---

[47] See the entries for the Duchess of Wessex and Duchess of York in Schedule 1.

[48] In "Celebrities' Non-Violent approaches to coping with Stalkerazzi" on *Netscape Celebrity* Stephanie Dubois sets out examples including Jennifer Aniston's injunction after "stalkerazzi" climbed her neighbour's eight-foot wall to photograph her sunbathing topless in her own back yard. Some tabloids are proud to be sued. In the edition of *Voici* for 16 – 22 July 2011 the tabloid boasts that the latest celebrity to sue is Vincent Elbaz (the article is sneeringly headed "Le martyre de Vincent Elbaz"). Next to this article is "Le top 5 des dommages et intérêts" of those who have obtained verdicts against *Voici* , noting these as: 1. Alice Taglioni 20,000 euros; 2. Jamel Debbouze 17,000; 3. Mélisse Theuriau 17,000; 4. Marie Drucker 16,000; 5. Christophe Dechavanne 8,000.

[49] http://graduateinstitute.ch/faculty/clapham/hrdoc/docs/echrvonhannovercase.doc .

> Privacy, on the other hand, is the right to be left alone. One has the right to be left alone precisely to the degree to which one's private life does not intersect with other people's private lives. In their own way, legal concepts such as libel, defamation, slander, etc. testify to this right and to the limits on other people's meddling with it. The German private-law doctrine of *Persönlichkeitsrecht* testifies to a broader concentric circle of protected privacy. Moreover, I believe that the courts have to some extent and under American influence made a fetish of the freedom of the press. The *Persönlichkeitsrecht* doctrine imparts a higher level of civilised interpersonal deportment.
>
> It is time that the pendulum swung back to a different kind of balance between what is private and secluded and what is public and unshielded.
>
> The question here is how to ascertain and assess this balance. I agree with the outcome of this case. However, I would suggest a different determinative test: the one we have used in *Halford v. the United Kingdom* (judgment of 25 June 1997, *Reports of Judgments and Decisions* 1997-III), which speaks of "reasonable expectation of privacy".
>
> The context of criminal procedure and the use of evidence obtained in violation of the reasonable expectation of privacy in *Halford* do not prevent us from employing the same test in cases such as the one before us. The dilemma as to whether the applicant here was or was not a public figure ceases to exist; the proposed criterion of reasonable expectation of privacy permits a nuanced approach to every new case. Perhaps this is what Judge Cabral Barreto has in mind when he refers to the emerging case-law concerning the balancing exercise between the public's right to know and the private person's right to shield him- or herself.
>
> Of course, one must avoid a circular reasoning here. The "reasonableness" of the expectation of privacy could be reduced to the aforementioned balancing test. But reasonableness is also an allusion to informed common sense, which tells us that he who lives in a glass house may not have the right to throw stones."

This decision was received with scorn even by respected news sources such as the *New York Times.* Doreen Carvajal[50] complained (wrongly) that the "so-called Caroline verdict" related only to the publication of five photographs, and that the judgment dangerously permitted privacy in public spaces for celebrities who wanted to block publication of unauthorized photographs. The article went on to criticize the Court:

> "In the United States the press is much more clearly protected by the constitutional right to freedom of expression… But in Europe, the Court of Human Rights concluded that there are limits to how the press can meet the public's fascination with the daily lives of the rich and famous."

Ms Carvajal went on to say that in the United States, the very fact that people want to know intimate details of celebrities' private lives offers enough justification under the Constitution for this to be provided. If this included Milly Dowler's family, could they be the target of similar inquiries on the basis the family members are limited purpose public figures?[51] Would the same intrusions into their privacy be permitted?

---

[50] "For the Famous, "Privacy" Even in Plain Sight", *New York Times,* October 10, 2004.

[51] Some judgments on limited purpose public figure appear inconsistent e.g. *Barry v Time Inc* 584 F. Supp. 1110 (D. Cal. 1984) (university head men's basketball coach a limited purpose public figure) and *Moss v Stockard* 580 A.2d 1011 (D.C. 1990). (university head women's basketball coach not a limited purpose public figure). However, I have assumed that a court would be likely to find the family limited purpose public figures.

The phenomenon of the shrinking and evolving newsroom is just as evident in the United States as it is in England. While 72.3% of Americans read the newspaper when *Gertz* and *Times v Sullivan* were handed down[52], by 2010 this had dropped to 46.3%. There is a similar drop for television. Americans today are obtaining their news from internet sites like the *Huffington Post* and *ProPublica.* Would American newsgatherers in search of a good front page story be tempted to hack into Milly Dowler's phone in the hope of a scoop or a scandalous piece of gossip that was certain to sell newspapers and if not, why not?

"I can't see it happening here" – phone hacking and the First Amendment

The response of many American journalists was summed up by Barbara McMahon in her *Guardian* article of 16 July 16, 2011 ("I can't see it happening here. To us, British tabloids are insane") as follows:

> "Most American media commentators think it unlikely the sins of the News of the World have been repeated here, citing major differences between US and UK cultures. While there is no equivalent of the Press Complaints Commission, journalists and editors are regarded as taking self-regulation more seriously. Reporters can be instantly dismissed for the smallest misdemeanor. The tabloid culture is kept separate from the hard news culture. US tabloids rarely break stories of importance and are therefore less powerful than in the UK."

Britain's strict libel laws have also been blamed[53].

There have been major wiretapping scandals in the United States involving the private lives of celebrities as well as investigative journalism; to take but one example, the scale of the Pellicano wiretapping, with its trillions of documents, involvement of corrupt officials, litigation on a mass scale, and physical attacks on journalists at respected journals such as the *New York Times*, is at least comparable in size and seriousness to the *News of the World* scandal today. Some journalists may have been involved, in that one of Pellicano's methods was to threaten publication if he was not paid money to bury the story. However, in the main, journalists came out of the Pellicano case quite well, as their investigation (especially Ms Busch's reporting) helped to bring his conduct to the attention of prosecuting authorities.

American mass media self-regulation represents a strong line of defence, but is this sufficient, especially in a world where journalists from less self-regulated jurisdictions may be operating on their turf? In the long term, it may be time to reconsider whether the First Amendment is sufficient protection. Since the early 1970s, judges[54], books[55]

---

[52] NEWSPAPER ASSOCIATION OF AMERICA, *Daily National Readership Trends*, http://www.naa.org/docs/Research/Daily_National_Top50_64-97.pdf.

[53] "Why Britain's Strict Libel Laws Actually Encourage Tabloid Antics", Time World, 13 July 2011. This article quotes an English media lawyer as saying that it is "almost an impossibility" for anyone to lose a libel action in England, and that anyone from any country can sue no matter how limited the publication. This is incorrect; see the libel statistics kept by *Inforrm* at their website.

[54] For example, the very timely warning in *Rosenbloom v Metromedia* 403 U.S. 29 (1971) where Byron White J said: "… technology has immeasurably increased the power of the press to do both good and evil. Vast communication combines have been built into profitable ventures. My interest is not in protecting the treasuries of communicators, but in implementing the First Amendment by insuring that effective communication which is essential to the continued functioning of our free society."

[55] See for example Robin D Barnes, "Outrageous Invasions: Celebrities' Private Lives, Media, and the Law", Oxford University Press, 2010;

and articles[56] have warned that the tidal wave of celebrity gossip has, thanks to modern technology, seeped through into conventional media channels, and that the First Amendment principles in *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), drafted at a time when celebrity was hard to achieve and electronic communication in its infancy, were an insufficient safeguard for a free press.

Robin D Barnes foresaw the problem in 2008:

> "The long-term implications of maintaining a free press under corporate domination, and in light of evolving technologies that impact public media generally, are ripe for constitutional analysis."

The growth of News International in the United States has coincided with a shrinking of media ownership generally. In 1983, 50 corporations owned most the US media (TV, radio, print, movies)[57]. By 1997, when technological advances had changed the nature of the media and deregulation had led to mergers and acquisitions, this number had reduced to 10. By 2009 there were 6 corporations with ownership of the traditional mediums, but there were many new media sources accessible through the world wide web[58].

Professor Robin Barnes gives one interesting example of illegally obtained material being used by American television programmes and the tabloid press, namely the August 1994 leaking of the Los Angeles Department of Children and Family services report on allegations about Michael Jackson to *Hard Copy.* Within hours of receiving the document, the California affiliate of a British news service sold copies to reporters for $750 each. The dramatic headlines of the story promised complete details of the allegations of the boy. Police investigating the matter had not yet determined to lay charges[59]. While the police were investigating, the boy's father filed a $30 million civil claim for sexual battery. In a good illustration of the global nature of tabloid news, Jackson's former employees, Stella and Phillip Lemarque sought to sell their stories through broker Paul Barresi, who negotiated a sale to *The Globe* in England for £15,000. Police never did lay charges, but Jackson's advisors, faced with the ruin of his career, settled the claims for enormous sums, which Professor Barnes notes (at p. 261) was characterized by Jackson's defence attorney 12 years later as very bad advice. Jackson's legal team were simply overwhelmed. It also cannot have been of assistance to Jackson that his lawyers consulted Antony Pellicano. What is also interesting about this case is the degree of involvement of the English press.

In addition, phone hacking stories where the wrongdoing occurred in England may first be published far away to hide the evidence. Alex Mitchell asserts this happened with the most notorious of all hacked conversations, the "Camillagate" tape which Mr Mitchell claims was first published in *New Idea* in Australia:

> "Old-school journalists who have an inside knowledge of darker newspaper practices will confirm that some stories are too hot to handle. In such circumstances the stories are fed to

[56] I note one only of the many articles on this subject, namely Jeff Kosseff, "Private or Public? Eliminating the *Gertz* Defamation Test", http://www.jltp.uiuc.edu/works/Kosseff/index.htm#_ftn1 .
[57] Ben Bagdikian, "The Media Monopoly", 1997.
[58] "Outrageous Invasions", p. 274.
[59] Seth Mydans, "No charges for now against Michael Jackson", *New York Times,* 22 September 1994.

overseas publications where they are faithfully reported so they can then be picked up and republished in their country of origin."[60]

Legislation

Similar legislation, rendering phone hacking unlawful, can be found in the United States, Australia and England. The legislation in England is discussed at length in the full parliamentary report on phone hacking[61] so I shall only briefly summarise it here.

The principal legislation in England is the *Regulation of Investigatory Powers Act* 2000 ("RIPA)[62]. After *Halford v The United Kingdom* (20605/92) [1997] ECHR 32 (concerning a police officer whose phone was hacked during proceedings against her employer for sex discrimination) showed the limitation of s 8 of the *ECHR,* Jack Straw, the Home Secretary, explained that the impetus for this new legislation was not only to extend this protection but also because "this revolution in communications technology is one of the imperatives for change in the law"[63]. Section 1 makes it illegal for any person intentionally and without lawful authority to intercept any transmission on a public (s 1(1)) or private (s 1(2)) communication whilst it is being transmitted. A person guilty of an offence under either provision would be liable for imprisonment of up to two years or a fine or both (s 1(7)). Section 79 deals with liability of directors of companies. Thus human rights legislation has an extension to protect privacy from illegal phone hacking.

An additional concern for corporations which form part of a multinational corporate group is that conduct which breaches the law in one country may lead to prosecution of not only in that country but in other jurisdictions in which it carries on business. For example, American legislation such as the *Foreign Corrupt Practices Act (FCPA)* may apply if, in the course of the phone hacking activities, payments considered to be of a corrupt nature were made to police by a corporation resident in the United States.

In addition, conduct of this kind may, in the future, fall within the provisions of the *Bribery Act* (UK), the commencement date for which is 1 July 2011. There are four key differences between this act and the *FCPA*, namely:

- it covers conduct between commercial entities, and not just conduct involving a government body or official;

- strict liability rather than proof of intent is required;

---

[60] http://www.smh.com.au/world/camillagate-scoop-raises-questions-for-murdoch-20110730-1i5cf.html . The *Sunday Age* made this claim at the time, in January 1993. Rupert Murdoch denied knowing the Australian publication *New Idea* had it, or had it published, and said he "wished he had". Mr Mitchell asks the pertinent question of whether legal advice was obtained at the time.

[61] http://www.guardian.co.uk/media/interactive/2011/jul/20/phone-hacking-news-corporation , chapter 2

[62] See also the *Data Protection Act* 1998; *Computer Misuse Act* 1990; *Bribery Act* 2010 (commencement date 1 July).

[63] See the review of this legislation in *Inforrm* by Adam Wagner: http://inforrm.wordpress.com/2011/07/12/opinion-was-in-human-rights-wot-won-the-phone-hacking-scandal-adam-wagner/#more-10414 .

- not only employees but persons "associated" with the company is sufficient;

- there is no distinction between bribery and facilitation – so lunches by the police at NI headquarters could be caught.

The *Bribery Act* was passed after the OECD put pressure on Britain to take steps to enact legislation similar to the FCPA; a 2005 report noted nobody in Britain had been charged with bribery in the previous six years[64].

In the United States, Federal and State statutes governing wiretapping and electronic eavesdropping are clear and succinct pieces of legislation.[65] Unauthorised retrieval of another's voice mail messages constitutes an interception (*Konop v Hawaiian Airlines Inc* 302 F.3d 868 (9th Cir 2002)).

It is not necessary to set out further discussion of the legislation in detail, but one point should be noted, and that is that although it is often overlooked, it is also a federal crime to disclose information obtained from illicit wiretapping or electronic eavesdropping: 18 USC 2511(1)(c). thus, not only the original wiretapper or electronic eavesdropper may be prosecuted, but all those who disclose information, where that can be traced to a disclosure by the original wiretapper or eavesdropper, with reason to know[66] of the information's illicit origins, may also be caught, except to the extent the First Amendment bans application. The interaction of First Amendment rights with illegally intercepted material is discussed in *Bartnicki v Vopper* 532 US 514 at 533 – 4 but cf *Quigley v Rosenthal* 327 F.3d 1044 at 1067 – 8 (10th Cir. 2003) and *Boehner v McDermott* 484 F 3d 573 at 577 – 81 (DC Cir 2007). In *Bartnicki* the court did not define "public interest" and limited the findings to the facts of the case[67]. Future judicial interpretations of *Bartnicki* may take a more restrictive view.

Legislation relating to eavesdropping in Australia has rarely been invoked in relation to journalistic activities. States and Territories in Australia have each passed legislation concerning electronic surveillance. In New South Wales the relevant legislation is the *Listening Devices Act* 1984 (NSW), the language of which is, according to Fullerton J in *DPP v Fordham* [2010] NSWSC 958 at [27] "neither Protean nor complex".

The "living in an electronic age" argument

---

[64] http://www.guardian.co.uk/business/2005/apr/03/theobserver.observerbusiness2

[65] The CRS Report for Congress "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping", G Stevens and C Doyle, summarises the Federal legislation and refers to State legislation, so I shall not set this out in any further detail.

[66] This might include wilful blindness. In "The Insider" (p. 262) Piers Morgan says: "Someone had got hold of [Kate Winslet's] mobile phone number - I never like to ask how – so I rang her." Ms Winslet responds "How did you get my number, I've only just changed it. You've got to tell me, *please.* I am so worried now; if the press get my number, then I have to change it."

[67] See the discussion of these issues in: http://heinonline.org/HOL/Page?handle=hein.journals/berktech17&div=32&g_sent=1&collection=journals .

What about the argument that we live in an age of electronic surveillance, that wiretapping is routinely used by law enforcement officials, and that hacking into phones by journalists is insignificant compared to government phone tapping?

The figures for authorized phone tapping in England (see p.3 fn. 8) are only a fraction of the *NOW* phone hackings. The same is the case in the United States. Official wiretap use in the United States has remained steady, despite 9/11, although it increased by 34% between 2009 and 2010. 80% involved drug cases and 68% were in three States alone. Terminated wiretaps in 2009 brought 4,537 arrests and 678 convictions and in 2010 brought 4,711 arrests and 800 convictions – not a bad result for the 2010 total of 3,194 wiretaps. Only one application was refused[68]. Nor is it the case that wiretapping is continually rising; the 2008 figure was down 14%[69]. These figures are instructive when compared to the phone hacking figures for *NOW*.

It must be said, however, that figures in other countries are very different. Wiretapping warrants in France, once granted in only limited cases, are now an increasingly common request made by magistrates and juges d'instruction. *Le Figaro* reported on 12 July 2011 that the number of wiretapping orders for 2010 was 43,000, an increase of 65% on the number of requests made four years ago. The number of wiretaps exceeds budget requirements and service providers are reported to have threatened to suspend services.

The reason for the proliferation of phone hacking by journalists in the United Kingdom, when such conduct is almost unheard of in other common law jurisdictions with similar media, laws and media markets, is hard to explain. Could it be that work practices, management style or cultural values in the United Kingdom have played some part in the development of this practice?

This brings me to the first question for discussion.

Question 1: What does the phone hacking scandal tell us about corporate governance problems for companies where crime has become endemic?

> "Ordinary people, simply doing their jobs, and without any particular hostility on their part, can become agents in a terrible destructive process. Moreover, even when the destructive effects of their work become patently clear, and they are asked to carry out actions incompatible with fundamental standards of morality, relatively few people have the resources needed to resist authority" (Milgram, 1974).

The circumstances in which *NOW* changed from a "good" news gatherer into a "bad" one because of the "wrong" conduct of people who worked there are likely to provide research material for white collar crime academics for a long time to come.

What are the warning signs to management, or regulators, or investigators, that an outwardly responsible business like this 168-year-old *grande dame* of the news print world had gone feral? Some of the warning signs may have been:

*** *NOW* staff were prepared to do business with criminals on a regular basis**

[68] http://www.mainjustice.com/2011/07/01/wiretap-use-on-the-rise/ .
[69] http://www.mainjustice.com/2009/04/27/wiretap-applications-down-14-in-2008/ .

I have set out a chronology of the extensive dealings between *NOW* and Southern Investigations (SI), an investigation firm run by Jonathan Rees and Sid Fillery[70]. How any *NOW* executive or journalist could have considered Rees an appropriate person to carry out investigations for a respectable business is hard to understand.

Rees carried out his well-paid work for the newspaper over the period 1989 – 1999 and 2005 – 2008, but was clearly in touch with *NOW* while he was in gaol, as he was able to persuade Alex Marunchak in June 2002 to use *NOW* trucks and staff to follow the detective in charge of investigating Rees for the Daniel Morgan murder. As set out in Schedule 1, when police complained to Rebekah Wade, she supported Marunchak, although the circumstances in which a criminal wanted a *Crimewatch* journalist (and the police officer in charge of investigating this criminal for murder) followed less than three years after Jill Dando's murder should have been a request to be dealt with cautiously.

*** These were not isolated requests but an extensive and planned course of work**

Rees generated hundreds of thousands of documents for his clients; police ended up with ¾ million documents in the inquiry, although most of these were not Rees' office records. The raid in March 2003 by the Information Commissioner's Office on a house owned by private investigator Steve Whittamore found more than 13,000 requests from newspapers and magazines to obtain confidential information. On 15 May 2005 Whittamore, fellow private investigator John Boyall (who took over *NOW* work from Jonathan Rees after Rees went to gaol for 5 years in 2000), retired police officer Alan King and communications officer Paul Marshall were sentenced for providing confidential information to the *Sunday Mirror* and *Mail on Sunday.* Figures about whom they had provided personal information included EastEnders actors and a transport union secretary. Whittamore told the New York Times that he worked for 19 *NOW* journalists and editors, but that *NOW* was only one of his clients.[71]

Search warrants issued for the prosecution of *NOW* royal editor Clive Goodman and private investigator Glen Mulcaire resulted in documents containing between 4,000 and 6,000 phone numbers, 91 mobile phone PIN codes, a recording of Goodman explaining to a journalist how to hack a soccer official's voice mail, and other documents indicating extensive phone hacking.

Similarly, documentation seized when Anthony "P.I. to the Stars" Pellicano was charged included 3.868 terabytes of data, the equivalent of two billion pages of

[70] A summary is as follows. In 2004 Fillery told Gillard & Flynn ("Untouchables", London, 2004, pp 276 - 283) he and Rees had started carrying out work for Alex Marunchak, of *News of the World* after meeting him at the Daniel Morgan murder inquest in 1988 (Rees was charged with this murder, along with the Vian brothers, and Fillery with conspiracy to pervert the course of justice, following this inquest). Marunchak continued to give them work up until Rees went to prison in 2000, and Rees returned to doing *NOW* work between the date of his release in 2005 and his subsequent denial of bail on the Morgan murder charge in 2008. The exclusion of "supergrass" evidence led to the collapse of the Morgan murder trial in March 2011: http://www.guardian.co.uk/media/2011/mar/11/news-of-the-world-police-corruption). See Schedule 1 for more details.

[71] http://www.ndtv.com/article/world/how-prince-william-harry-phones-were-hacked-by-tabloid-48943

double-spaced text. There were tapes and transcripts of a telephone calls for film stars, such as Nicole Kidman. Pellicano's method was to record everything, but to listen only to those portions of the tape identified by sophisticated software as containing key phrases or raised voices. Although many victims were not informed, some found out, and their cases are being case-managed in the Los Angeles Superior Court by Judge West. Pellicano is serving a series of sentences which will expire in 2019.

*** The response is to cover up**

In the case of *NOW,* the wrongdoers may have been on the factory floor, so to speak, but those who had to answer for it were the management and senior management. A number of their statements (most recently, the press release for NI dated 10 July 2011) are set out in Schedule 1.

On 11 March 2011 Chris Bryant MP told the House of Parliament he had been warned off investigating the phone hacking scandal, and that he had also learned that 8 members of parliament were victims. Mr Bryant MP went on to state:

> "Almost as bad as the original illegal activity – only the tip of which we have yet seen – is the cover-up."

*** Lengthy litigation**

Elle McPherson sacked her business manager, Ms Field, in 2005, prior to the revelations in the 2006 - 7 Mulcaire trial that Ms McPherson's phones had been hacked. *NOW* and its lawyers must have been aware of Ms Field's problems soon after, as she appears to have been in touch with them ever since. Her claim for damages is pending before Vos J. She gave this interview to the ABC in May 2011:

> "MARK COLVIN: And have you had reason in recent weeks to be concerned about anything?
>
> MARY-ELLEN FIELD: Yes, very. After the last case conference on May the 20th there was a lot of publicity here in Australia about it and I gave a number of interviews including Sky News who unbelievably have been you know very fair. And my son called me, my younger son called me from work and he said, "Oh mum did you put something on my Facebook page? Did you post that interview on my Facebook page?" And well I don't even know what his password is and I said no. So he came home to see us that night and opened his Facebook page and there was an interview with me on his Facebook page, claiming that it had been posted by Tim, my son. And then I thought well sometimes Tim uses my laptop when he comes home to bring his washing home and things, that somehow it had migrated and I asked some friends who are in the IT industry and they said no, that's not possible. So I called the police, the police lady who's supposed to look after me. And she said (gasps) that must be a virus.
>
> MARK COLVIN: Yes it doesn't sound, from what I know of viruses it doesn't sound much like a virus.
>
> MARY-ELLEN FIELD: Well it's not a virus. So I…
>
> MARK COLVIN: So what happened when you went to Apple
>
> MARY-ELLEN FIELD: Well Apple were amazing. By that time, by the time I'd got that for three more items had been posted on Tim's Facebook page including what they were doing was taking links, or whoever it is, the links that I was sending, including the one I sent to you, people that

update you on what was happening, they appeared on Tim's Facebook page. So we went to Apple…

MARK COLVIN: So it may have come from an email you sent to me

MARY-ELLEN FIELD: One of the stories, one of the links I sent to you was then posted on my son's Facebook page. It didn't mention you but it was the same article, it was a link I'd sent you to an article that was in the Independent. So Apple were unbelievable. I rang their Irish, here you go to their Irish sort of service centre and they said come straight in tomorrow morning. So I went in there. They gave me a two-hour slot and brought my iPad and my MacBook and my iPhone and they gave me a brand new iPhone for no charge. They checked everything. They put some very complicated spy ware onto my Mac and said that it wasn't a virus. You know they couldn't find it but it was clearly a targeted attack because things can't migrate and said that you know we have to change our passwords very regularly, put you know alpha-numeric codes and change it regularly. But the fact is if someone wants to access something like this these days they can and everything we're hearing about the attacks on these major corporations and the IMF and things, you know just a little person at home, you know they're not very safe from these sorts of things.

MARK COLVIN: And I believe you've also got some evidence that somebody's interfering with your phone by sending calls when you're not there.

MARY-ELLEN FIELD: Yes. I'm seeing the policewoman who looks after me tomorrow, my husband and I are seeing her because it's affected my husband's phone and mine so…

MARK COLVIN: What happened? The phone rang, your phone rang your husband while you were in the bath and it was on the charger

MARY-ELLEN FIELD: Yes. And then, and my husband had walked down the street to go have a coffee. and he rang me and I, well because it was three rooms away where the phone was charging and he said, "Oh, sorry I missed your call." And I said, "I didn't call you." And then when I looked at my, there was an outgoing call from my phone and I couldn't, I wasn't near the phone, I was in the bath."

Ms Field went on to agree with Mark Colvin that this was "intimidating" but said that nothing could hurt more than what she went through in 2005 when she lost first her job and then her career after she was suspected of leaking confidential information about her client.

Conclusions: Are new rules for necessary for corporate governance, corporate ethics do ensure responsibility in keeping and accessing electronic publication?

Until the fact findings from the current inquiries are in, it is hard to say what lessons there are for corporate regulators, investigators and company managers arising from the apparent moral as well as economic collapse of the *NOW* business.

Can company management tell in advance when the wrongdoing of its own employees is such that the company might have to go out of business? How does a corporate business culture can turn into a criminal one? Are there warning signs that company employees' crime levels are about to become endemic? Although it is too early to say, some potential warning signs might be:

1. **Management should know there is a problem when your employees are spying on each other**: As the chronology in Schedule 1 sets out, Rees and Fillery were asked to spy on *NOW* employees and even senior managers like Andy Coulson and Rebekah Wade were phone hacked.

2. **Management should know there is a problem when company starts hiring/dining out with the people supposed to be investigating the company:** This has been the subject of a great deal of parliament debate (Hansard debates 10/3/2011 pt 0004, Chris Bryant MP). A variation would be publicly attacking these persons, insulting them, or calling for their removal[72]

3. **Management should know there is a problem if staff are developing "dangerously close" (Hansard debates 10/3/2011 pt. 0004) relationships with police officers and/or persons in organized crime**: The circumstances in which *NOW* resources were used to follow the detective in charge of investigating Jonathan Rees (see Schedule 1), in June 2002, when Rees was in gaol for a serious criminal offence, should have been a red light to company management (and the company lawyers) that *NOW* was losing its bearings, especially since police complained about it at the time to Rebekah Wade.

What about the victims of phone hacking? What kind of action should they bring, and in what court?

Question 2: Where an individual's right to privacy has been breached, is any remedy a claim in tort, a claim for breach of confidence, a claim for damages under data protection legislation, criminal compensation or a combination of the above?

In common law jurisdictions such as Australia and England, the development of privacy law has been left to judges on a case by case basis, in accordance with common law principles. In Australia, these cases have been very few in number, unlike the rapid development of this cause of action in England[73].

The High Court of Australia held, in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, that there was no common law right to privacy. The modern development of privacy law in Australia starts with *Lenah Game Meats v ABC* (2002) 208 CLR 199 . The facts in this case essentially were that a trespasser (probably an animal liberationist) filmed the killing procedure used in a possum factory, and sent this footage to the ABC. In other words, this was material obtained illegally and may have involved conduct of a "blagging" variety for the person who filmed it to get onto the property. In the course of setting aside the Tasmanian Court of Appeal's judgment restraining broadcasting of the material, members of the High Court made *obiter* statements (at [106] – [108], [111], [132], [187] – [189]) to the effect that *Victoria Park* did not stand for such a proposition, and "*does not stand in the path of the development of such a cause of action"* (at [107]). This tantalizing proposition has remained up in the air since that time, although there have been judgments where damages for breach of privacy have been awarded.

[72] http://www.independent.co.uk/news/people/profiles/who-is-mr-justice-eady-2149371.html and http://www.publications.parliament.uk/pa/cm200910/cmselect/cmcumeds/362/36204.htm .

[73] See the discussion of the history of privacy law by Mr Justice Eady in "Strasbourg and sexual shenanigans: a search for clarity", March 11, 2010, available at http://www/indexoncensorship.org/tag/mr-justice-eady.

The first case in which such damages were awarded is *Grosse v Purvis* [2003] QDC 151. The plaintiff and defendant had a brief sexual relationship following which the defendant (whom the judge found remained infatuated with her) loitered near her home or attempted to contact her. There were 70 particulars of stalking, of which 35 had corroborating evidence from other witnesses, which Skoien DCJ considered (at [340]) supported this contention. In awarding compensatory damages of $180,000, aggravated compensatory damages of $50,000 and exemplary damages of $20,000, Skoien DCJ noted (at [420]) that stalking was a criminal offence pursuant to s 359B *Criminal Code* (Qld). Skoien DCJ observed:

> "It may be relevant to note that in perhaps all of the offences contained in the Code in which an individual person would be named in the indictment as the complainant (or victim) an actionable tort is encompassed so that the victim would have the right to sue in the civil court for damages. One might ask why would that not also apply to a new offence like stalking in which the victim suffers personal injury or other detriment?"

A preliminary issue, when determining the parameters of any action for damages for breach of privacy, is the nature and extent of any criminal conduct upon which the claim for damages is based and how this impacts on the nature of damages and the defences to be pleaded to such an action.

The right to damages for invasion of privacy is still in its infancy in Australia; the entitlement to bring such an action is not in doubt in England or in the United States. However this brings me to the next problem, which is that, in England, there is no consensus as to whether tort law principles, or equitable principles (as an extension of principles governing the law of confidence) should apply[74]. Claims for damages arising from publication of private material may arise on occasions where there is a breach of confidence, a tortuous act and/or breach of statutory duty.

In English decisions, where claims are brought for the misuse of private information, the balancing exercise of the rights between the parties is not necessarily referable to issues of freedom of speech applied in defamation actions or principles of duty of care applied in tort actions, but rather by applying an "intense focus" to the facts of the case, and turn on issues of proportionality: *Campbell v MGN Ltd* [2004] 2 AC 457.

Mr Justice Eady explains this as follows[75]:

> "The truth may be simpler, namely that the law of privacy is a new creature deriving from the Strasbourg way of doing things, thus requiring language and terminology of its own. The new cause of action may not be classifiable as a tort because the balancing exercise is not about wrongs but about rights. If you are ordered not to do something, or to pay compensation for having done it, because it is not regarded as necessary and proportionate, that is quite a different concept from the court ruling that a legal "wrong" or "tort" has been committed. At least until the judge has carried out the required balancing exercise, it may be said in a real sense that no "wrong" has been committed. It is in the nature of the new technology that there are no absolute answers. It all depends on the facts."

[74] Mr Justice Eady (ibid) notes that McGregor on Damages at [42.47] categorises it as a tort, while Clerk & Lindsell on Tort at [28.03] think it is an extension from equity, but cover it in their textbook just in case.
[75] Mr Justice Eady, *ibid*.

Mr Justice Eady goes on to note that the very different balancing act required for this kind of cause of action may spread into other areas such as defamation, and the role of proportionality may be a factor to take into account, resulting in losing the reasonably clear black and white distinctions of truth and falsehood in defamation law, and that this may already be occurring in the context of interim injunctions. Whether this occurs or not, it underlines how important it is to distil the elements in the balancing equation in actions where the key claim is not the falsity, but the fact that the information is made public.

An additional area of concern is the availability of interim and permanent injunctions, especially "superinjunctions"[76] and injunctions "contra mundum".

What kind of tribunal should hear these claims?

If there are thousands of victims, then this is likely to lead to a large number of cases. It may be appropriate to consider alternative forms of relief for the victims, especially where claims are small or the victims' financial means are limited.

Alternatives to proceedings in the Queens Bench courts might be:

- Where the conduct complained of is criminal in nature, the jurisdiction of criminal compensation boards, such as the Criminal Injuries Compensation Authority (CICA) in England, could be extended. The amount awarded could then be enforced against the wrongdoer by the compensation authority, which would then enforce the judgment against the wrongdoers;
- The establishment of a special tribunal, a proposal put forward by Hugh Tomlinson QC but rejected in the PM Privacy Commission Report[77];
- Greater use of the PCC;
- Class action case management procedures, of the kind used by the California courts to manage the Antony Pellicano wiretapping litigation.

Use of criminal injury compensation tribunals

The Criminal Injuries Compensation Authority (CICA) provides payment of limited amounts to victims of violent crime. The advantages of such a scheme are the costs savings, and that the matter would be resolved without the victim having to confront a large legal team representing a media defendant. It would also be a proactive way of forcing victims of such practices to complain to police, or otherwise put the wrongdoer in a position where the wrongful conduct is likely to come to official attention, which would be a way to keep a check on future illegal conduct and discourage secret settlements such as the Taylor £700,000 settlement. The question of what amounted to suitable damages would be a question for the Authority, not the media. Applicants could receive compensation more quickly and cheaply than would be the case in the event of a complex action for loss of privacy. The burden of proof is civil, not criminal. An interesting problem would be how to obtain the evidence if the police decided not to prosecute.

[76] See Heather Rogers QC's article in *Inforrm*, 26 November 2010.
[77] The PM Privacy Commission Report, 22 July 2011, at 13.

This would not prevent persons bringing an action for damages in a privacy-related action where the conduct involved was not criminal, or the damage substantial. A defendant in those proceedings could, of course, bring a summary application on the basis that the conduct was criminal, but since offering to be prosecuted instead of paying common law damages is an unattractive proposition, such applications are likely to be rare. It may be that, if there are many victims of phone hacking, a system of payments of this kind (with the judgments consequently enforced against the media company and/or journalist personally) is a better alternative to hundreds of cases being individually managed for years.

Setting up special tribunals, conditional fee agreements and the role of the PCC

The PM Privacy Commission Report issued on 22 July 2011 noted that Hugh Tomlinson QC has suggested:

> "It seems to me it's in everybody's interest to have a press that is dynamic, free, interesting and active and keeps to the basic rules. And the question is how you can best do that at the least expense in the public interest and it seems to me that actually a system of tribunals away from the huge expense of the courts would be a positive outcome."[78]

Sir Charles Gray (who is in charge of the compensation scheme set up by NI[79]) suggested that this proposal might be worthy of further consideration, but the Report authors did not agree either with this suggestion, or with the use of conditional fee arrangements to assist claimants with limited funds.[80] The Report authors did, however, consider:

> "We recognize that the PCC can demonstrate success in working with individuals who would otherwise have no support and believe this should be an important part of any new regulatory arrangement or other industry wide initiative. The availability of this support needs to be advertised more widely."[81]

The Commission does not analyse the PCC's complaints findings, or expose its reasoning for believing, in circumstances where the PCC utterly failed to deal with both general complaints of phone hacking (by the *Guardian*) or individual complaints by victims, it would somehow be able to continue to do so in the future. Nor is it the case that the availability of the PCC needs to be advertised more widely. According to the PCC's 2006 annual report, for example, the number of complaints to the PCC outnumbered the number of press complaints to the court for the same period. 231 of the 3,325 complaints related to privacy and PCC chairman Sir Christopher Meyer told the *Press Gazette* (27 April, 2007) that despite what were called "recent rulings apparently strengthening privacy law", the PCC remained the "only place to go" with complaints. Far from being concerned about lack of knowledge about the PCC, Sir Christopher said:

> "People think the shift is going to be away from the PCC to the courts because of this sequence of decisions. But far from seeing a [decrease] in the number of privacy complaints we have investigated and resolved more than we have ever done."

---

[78] The PM Privacy Commission Report, July 22, p. 13.
[79] http://www.guardian.co.uk/media/2011/jul/07/news-of-the-world
[80] *Loc. cit.,* p. 14.
[81] *Ibid,* p. 14.

Sir Christopher went on to warn against efforts by "governments and judges to curb journalists' freedom of expression", adding that the threat was "real" and that if "the trend" continues, there will inevitably be calls for a First Amendment freedom of speech defence. He went on to add that the results of the PCC investigation into *NOW*'s royal editor Clive Goodman was "going well" and it would be published in May 2007. (It would be interesting to know just how much documentation the PCC actually looked at).

Is this the language of an independent tribunal? I am not sure what government attempts he is referring to, but the "judges" reference is probably another slight on Eady J.

A recommendation of warning of publication was also supported, but the Commission was not convinced that the imposition of a legal requirement for prior notification was the right way forward. It does not sounds as though getting both sides of the story, which is considered such an important part of qualified privilege defences in Australia, plays very much part in the minds of the Commission.

The suggestion made by Hugh Tomlinson QC has a lot to commend it. Such a Tribunal could deal with small claims, ensure corrections are published and report breaches of the law to appropriate authorities. Litigants could, in straightforward cases, represent themselves, much as they have done before the PCC, and a pro bono or legal aid lawyer be assigned to more difficult cases. Claims above a certain threshold could be referred to the court for determination.

Whether or not such a tribunal is set up to deal with privacy complaints or small damages claims, it would still be preferable if an independent tribunal took over the work of the PCC. Board members could include retired journalists (with no conflict of interest problems), respected community members and/or academics in the journalism field.

The California Complex Court pilot programme

Another alternative would be to treat actions arising from, for example, the Mulcaire hacking, as a class action, and to manage them in the same way the California Complex Court pilot programme is used to manage the Pellicano litigation (where many of the plaintiffs complain about wire tapping). Again, this would reduce legal fees and give claimants a more level playing field, as well as reducing the pressure on the courts.[82] This is particularly likely to be the case if there are any actions brought against the telephone service providers, as is currently the case in the United States[83] The case management system set up by Vos J for case management of the hacking claims may, however, be more appropriate for the English legal system.

At least one of the hacking victims, Jude Law, has commenced proceedings for a publication to which the law of the United States applies. Clearly this is likely to be an issue for further consideration in the future.

---

[82] For information about the California Complex Court program see http://www.flcourts.org/gen_public/cmplx_lit/bin/reference/Other%20States/California/california%20deskbook%20excerpt.pdf; and http://www.kbklawyers.com/news/ladj_complcourts.pdf .

[83] http://www.thedaily.com/page/2011/06/10/061011-gossip-anita-busch-1-2/ .

Question 3: What are some of the issues the UK inquiries should look into?

Lord Justice Leveson, who will conduct the phone hacking inquiry, has indicated there will be a series of public discussions and lectures in which the scope and content of the conduct to be examined will be discussed. The terms of this inquiry are not fixed in stone, and Lord Justice Leveson has already expressed concern about meeting the deadline[84].

For those reasons, the third question for consideration during this UIA conference session is the question of what areas of the phone hacking scandal are matters which, from the point of view of those participating in this session, might merit further inquiry. (Although there are a number of inquiries on foot, the one most likely to be of interest is the inquiry headed by Lord Justice Leveson). To start the ball rolling, I have set out some suggestions of my own.

The need for a review of press standards and media regulation

Lord Justice Leveson has indicated that questions of media ethics and standards will be part of the area for consideration of reforms.

This is an enormous topic, so it may help to identify the problems by looking at how the media has dealt with stories in one particular area. The area of reporting about which *NOW* was most proud was its series of articles concerning child sex abuse, such as the campaign for "Sarah's Law" and articles by Mazher Mahmood exposing child sex abuse. If there are high journalistic standards to be found, it should be in this area.

Some troubling issues in relation to articles in *NOW* on child sex abuse include:

- Leaving aside the controversy concerning the appropriateness of Sarah's Law, not only an MP opposed to the law but even Ms Sara Payne, the mother of the murdered child, had their phones hacked;

- *NOW* published articles about celebrity child molester allegations, such as the August 1994 allegations about Michael Jackson (for which he was never charged) while failing to give any or any significant coverage to the large numbers of court proceedings involving Catholic clergy. According to Jason Berry & Andrew Greely[85], American dioceses had paid out at least $500 million in damages and the eventual costs would exceed $1 billion; in 1993

[84] http://www.guardian.co.uk/media/2011/jul/28/phone-hacking-inquiry-leveson .

[85] "Lead Us Not Into Temptation: Catholic Priests and the Sexual Abuse of Children", 2000.

one attorney was prosecuting 200 active Catholic clergy sex abuse cases in 27 States[86];

- While Mazher Mahmood boasted of his role in putting many pedophiles behind bars, the collapse of the Gary Glitter trial after revelations the victim had been paid by *NOW* let the accused person go free. He was subsequently expelled from Sri Lanka and sentenced to imprisonment in Vietnam for similar offences. One of the persons who worked with Mahmood, Sid Fillery of Southern Investigations, was himself convicted of possession of child pornography in 2003.

This is part of a wider problem of reporting crime generally. While a recent example is the contempt of court proceedings and tabloid libel settlements concerning coverage of Chris Jeffries in the Jo Yeates murder case[87], this has been a problem of long standing[88] not only in England[89] but in Australia. Pressures on politicians in New South Wales not to be "soft on crime", particularly from talkback radio, have resulted in New South Wales having the highest (or equal highest) statutory maximum penalties for a number of offences, a higher rate of imprisonment than the Australian average, and a higher proportion of offenders sentenced to full-time imprisonment[90].

Questions for the police inquiry

Here are some questions that occurred to me while preparing this discussion paper. The relevant dates for these are set out in the Schedule 1 chronology.

1. What happened to the referral to the Attorney-General of News of the World in the Victoria Beckham case by Judge Simon Smith in June 2003?

2. According to the *Times*, Rees and his colleagues (which would have included Marunchak) faced a police investigation in relation to the Pure Energy and Pure Electricity scams in 2005. What happened?

3. What went wrong with the 2006 phone hacking trial before Judge Darlow?

4. Use of telephone intercepts and leaking information to the press in proceedings brought by police officers for wrongful dismissal.

---

86 "The Sexual Abuse of Children in the Roman Catholic Archdiocese of Boston: A Report by the Attorney-General", July 23, 2003. Both these references are taken from Professor Robin Grimes, *loc. cit.,* p. 260.

87 http://www.pressgazette.co.uk/story.asp?storycode=47607

88 For example, calling for the sacking of 10 English judges on the basis that they are "soft" on crime: discussed by Emma Bell in "New Guests in the Corridors of Power" available at: http://osb.revues.org/452#bodyftn45 (paragraph 15). See also the *Sun*'s complaints that Leveson LJ, among others, is "soft" on crime: http://www.thesun.co.uk/sol/homepage/news/3496327/Judges-No-jail-for-dealers-caught-with-50-heroin-wraps.html .

89 See the Attorney-General's concern over "frenzied" crime coverage in England: http://www.pressgazette.co.uk/story.asp?storycode=46828 .

90 "Full-time imprisonment in NSW and other jurisdictions", Judicial Commission of NSW, February 2007. The countries for comparison were the United States, New Zealand, England and Wales. Prior to the most recent State election, the chief judges of all three court tier levels in NSW made a public statement asking for law and order issues about length of sentencing not to become an election issue.

Examples are:

(a) Assistant Chief Constable Halford of the Merseyside Police, whose office phone was the subject of surveillance while she was bringing proceedings for sex discrimination: http://www.bailii.org/eu/cases/ECHR/1997/32.html.

(b) Sergeant Gopal Virdi brought proceedings for wrongful dismissal in the course of which material was leaked by the police to the Daily Mail. The majority of the £150,000 compensation awarded to Virdi by the employment tribunal related to the conduct of the police by leaking documents to the *Daily Mail.* A Metropolitan Police Authority report confirmed police had leaked documents including correspondence about settlement negotiations. Gillard & Flynn point to similar conduct in relation to Detective Constable Sarah Locker, and to the recording of conversations between Superintendant Ali Dizaei and his lawyer[91]. At one stage more than 3,500 of his calls were monitored (albeit legally).

(c) Persons working on the Steve Lawrence Inquiry claim that the leak of their report to the *Sunday Telegraph* on 21 February 1999 was because their offices had been "bugged" and "burgled" by police, who had then provided it to the media. Gillard & Flynn set out the evidence in chapter 17 of "Untouchables". Gillard & Flynn also claim that Duncan Hanrahan "would also have been of great interest to the Lawrence Inquiry" (at p. 305) if those conducting it had known what he had to say. Hanrahan, a private investigator whom Gillard & Flynn say did work for Alex Marunchak, was one of the "supergrasses" in the collapsed Morgan murder trial.

(d) A proper inquiry, headed by a judge, into the murder of Daniel Morgan. The conduct of police, journalists and private investigators which led to miscarriages of justice should be at the forefront of the investigation. Some of these matters, such as the murder of Daniel Morgan (see Schedule 1) are so serious that they require their own investigation.

5. Mary-Ellen Field – Elle McPherson sacked her lawyer, Mary-Ellen Field, because she believed Ms Field had leaked information about her. Ms Field's career was ruined and her health affected. Although evidence that Elle McPherson's phone was hacked was discovered during the Glen Mulcaire trial, her requests for assistance from the police appear to have been ignored, which may warrant inquiry. Ms Field's subsequent legal and other difficulties, which have received extensive coverage in the Australian media and in particular by the ABC, includes allegations of being electronically spied on as late as May 2011.

[91] Gillard & Flynn, *loc.cit.,* Chapter 26.

6. Victoria Beckham, and the persons accused of attempting to kidnap Victoria Beckham – David Beckham has said he believes he has been the target of phone hacking over most of the past decade[92], but the most serious incident involving the Beckhams should be the circumstances in which *NOW* staff caused the police to arrest and charge persons for plotting to kidnap Victoria Beckham. This was one of the Mazher Mahommod's entrapment cases. The case collapsed largely because of evidence of payment of £10,000 to a witness, but the weak evidence, and the manner in which the defendants were lured and tricked by the *NOW* were also noteworthy. Judge Simon Smith referred the matter to the Attorney-General and inquiries should be made as to what happened to this referral, especially as it was one of a series of trials which collapsed because of the conduct of *NOW* journalists. The PCC self-referred the matter, but decided in favour of the *NOW*. They took no steps to discourage this practice, although in an article "Chequebook journalism in the dock", (3 June 2003) the BBC noted the collapse of the 1999 Gary Glitter indecent assault trial where a witness was paid a similar sum. The BBC also noted there were payments to witnesses in the Rosemary West trial.

7. Criticisms of judges who have handed down judgments on privacy issues – In Schedule 1 I have set out some statements by Rupert Murdoch and others expressing great fears about the introduction of a tort of privacy. This fear is not restricted to *NOW*. In 2008 Paul Dacre made a speech to the Society of Editors calling Eady J's judgments "arrogant and immoral" and saying he was "inexorably and insidiously" introducing a privacy law through the back door. This may be an area for further inquiry, as may calls for the sacking of judges seen as soft on crime (see the reference to Emma Bell's article at footnote 88).

8. The Australian Prime Minister, Julia Gillard, has indicated that she is prepared to hold a media inquiry to consider, among other issues, privacy law, and the Greens leader, Bob Brown, has called for a review of media ownership. There may also be inquiries in the United States. There should be exchange of information between these inquiries.

9. Whether this conduct is restricted to *NOW* - Mr Dacre, editor of the *Daily Mail*, described how he and had dinner with Gordon Brown to warn about the danger of amendments to the Data Protection Act to increase penalties for phone hacking:

> "About 16 months ago, I, Les Hinton of News International and Murdoch MacLennan of the Telegraph, had dinner with Gordon Brown and raised these concerns. We also raised a truly frightening amendment to the Data Protection Act, winding its way through parliament, under which journalists faced being jailed for two years for illicitly obtaining personal information such as ex-directory telephone numbers or an individual's gas bills or medical records. This legislation would have made Britain the only country in the free world to jail journalists and could have had a considerable chilling effect on good journalism. The prime minister - I don't think it is breaking confidences to reveal - was hugely sympathetic to the industry's case. Whatever our individual newspapers' views are of the prime minister - and the Mail is pretty tough on him - we should, as an industry, acknowledge that, to date, he has been a great friend of press freedom."

[92] *The Sunday Telegraph,* 17 July 2011.

10. The circumstances in which police followed up on NOW surveillance of *Crimewatch* reporter Jacqui Hames, and whether NOW reporter Alex Marunchak received information from Rees about the murder of Jill Dando.

Conclusions

The challenges of technological development – not only surveillance equipment but social media where boundaries for privacy are challenged – are central to the debate of the right of the press to public private information for financial gain which is the subject matter of the phone hacking debate. In recent years, technology "has immeasurably increased the power of the press to do both good and evil. Vast communication combines have been built into profitable ventures", as Byron White J pointed out in *Rosenbloom v Metromedia*.

More than thirty years ago, Britons were warned:

> "The battle lines are already being drawn for the struggle to control information in Britain. Government administration, worker collectives, corporations, police and security forces, and foreign corporations and Governments all seek to preserve their own privacy while finding out as much as possible about everyone else. Information is at the commanding height of tomorrow's economy."[93]

The question is how to regulate the sale of personal information so as to keep appropriate boundaries for the privacy that is an instinctive part of our social structure. Where those barriers should be placed are questions of social and moral as well as legal importance, as the public response to the hacking of Milly Dowler's phone demonstrated.

The issues for discussion need to go beyond the illegal conduct of phone hacking, and to focus on questions of freedom of the press. This is yet another occasion to draw attention to the research of Professor Vai Io Lo and Xiaowen Tian showing that freedom of the press is a more significant control on corruption than elections – in fact, it is more successful in this regard than democracy itself[94]. However, that freedom can be challenged just as easily by bad journalism as it can by oppressive regulation.

[93] The farseeing author(s) of this statement will be revealed at the conference.

[94] Xiaowen Tian and Professor Vai Io Lo in "Conviction and Punishment: Free press and competitive election as deterrents to corruption", (2009) 11 *Public Management Review* 155 – 172 at 156.