Social media issues for investigators

Judith Gibson[1]

Australian Institute of Professional Investigators

11 November 2015

Introduction

One in seven people on the planet (i.e. one billion people) consult at least one social media source - Facebook - every day[2]. Social media has had an impact on every sector of our society – not only in business, or in the legal profession, but our lives at the most personal level.

The following examples demonstrate some of the areas which have been impacted. In its 2014 report,[3] Deloitte stated that reputation damage from online (especially social media) attack or criticism was identified as a primary risk by 90% of the business operators who responded to their survey, an indication of the concerns at business level. Government and community organisations are anxious about social media use for criminal or terrorist activities, and police maintain an active social media presence. At the family or individual level, the Commonwealth Government has introduced legislation aimed at cyberbullying attacks on children, for which the source is largely social media[4].

All these problems have one source: the ability of anyone using the Internet, and in particular social media, to publish their opinions and views – the good, the bad and the ugly – to the

---

[1]Judge, District Court of New South Wales; contributing author, Tobin & Sexton, "Australian Defamation Law and Practice" (LexisNexis). All internet links were last accessed on 8 November 2015.

[2] Facebook, set up in 2004, gained its billionth user in 2012: "Facebook has over a billion users in a single day, says Mark Zuckerberg", *BBC News*, 28 August 2015 (http://www.bbc.com/news/world-us-canada-34082393). The phenomenon of 1 billion users a day (1 in 7 people on the planet) was first achieved in August 2015. Facebook now averages 1 billion users a day: Sam Thielman, "Facebook now averages over one billion users a day", *the Guardian*, 5 November 2015 (http://www.theguardian.com/technology/2015/nov/04/facebook-one-billion-users).

[3] "2014 Reputation Risk Survey", Deloittes, http://www2.deloitte.com/us/en/pages/governance-risk-and-compliance/articles/reputation-at-risk.html.

[4] The *Enhancing Online Safety for Children Act* 2014 (Cth) took effect from 1 July 2015. Former Australian Federal Police cybercrime expert, Alastair MacGibbon, has been appointed e-Safety Commissioner. According to nobullying.com, 463,000 Australian children were affected by cyberbullying during 2013. See Corrs, "Australia's new cyberbullying watchdog", 17 April 2015, http://www.corrs.com.au/publications/corrs-in-brief/australias-new-cyber-bullying-watchdog/

world at large, where the permanent nature and often anonymous origin of these social media publications cause problems for everyone from corporations to law enforcement to vulnerable teenagers victimised by social media trolling or bullying.

In countries such as the United States, law firms and investigation companies with dramatic names (e.g. "Internet Defamation Removal Attorneys"[5] and "Cyber Investigation Services"[6]) have sprung up, offering to investigate and remove offending material such as fake online reviews[7], social media cyberbullying[8] and reputation-damaging snippets.[9] Whatever the source of the social media problem (and it can come from an employee's "own goal" just as easily as from an anonymous cyber-attack),[10] cyber reputation damage is big business in many countries around the world.

Social media's importance for investigators does not arise because of this lucrative new business of reputation management; reputation damage investigation is just a useful addition to services offered for clients. It is the ease with which previously confidential information can be obtained from social media sites, as well as entirely new kinds of information from analysis of mass data, which make social media a vital investigative tool.

Social media can also provide a forum for investigators to make their findings publicly available at no cost. When Elliott Higgins[11] started tweeting from his lounge room about troop movements in Syria, nobody predicted that this unemployed IT specialist would become one of the most respected troop movements experts in the world. Social media's low barriers include sharing investigative techniques, as can be seen by Mr Higgins sharing his investigative techniques with anyone interested, by posting on social media and YouTube. Similarly, the International Consortium of Investigative Journalists ("ICIJ')[12] has not only

---

[5] Their website can be found at http://www.defamationremovalattorneys.com/.

[6] Their website can be found at http://www.cyberinvestigationservices.com/protect-reputation-brands/.

[7] Cheryl Conner, "Online Reputation: New Methods Emerge For Quashing Fake, Defamatory Reviews" *Forbes*, 30 October 2013, http://www.forbes.com/sites/cherylsnappconner/2013/10/30/online-reputation-new-methods-emerge-for-quashing-fake-defamatory-reviews/.

[8] As at January 2012, there was legislation against cyberbullying in 48 States in the United States: Dena T. Sacco, Katharine Silbaugh, Felipe Corredor, June Casey and Davis Doherty, "An overview of State Anti-Bullying Legislation and Other Related Laws, (http://www.meganmeierfoundation.org/cmss_files/attachmentlibrary/State-Anti-Bullying-Legislation-Overview.pdf).

[9] For a self-help guide to removal of material from Google, see https://support.google.com/websearch/troubleshooter/3111061?hl=en .

[10] For a list of the 50 top social media risks, see "50 Ways social media can destroy your business (https://blog.kissmetrics.com/social-media-can-destroy/).

[11] The Bellingcat site, set up by Elliot Higgins, can be found at https://www.bellingcat.com/author/eliothiggins/

[12] Their website can be found at http://www.icij.org/.

provided remarkable investigative reports on offshore tax havens and financial fraud around the world, but has shared its investigative methods and report-preparing skills online[13]. Prosecuting offshore tax haven account holders is an expensive and at times fruitless task; having journalists investigating (and then naming and shaming) the rich and infamous is an easy alternative for harassed and underfunded governments unsuccessfully battling financial corruption. While it could not be said that investigation is replacing prosecution, the reports of ICIJ must at least give law enforcement officials an advantage.

Additionally, use of social media has made the work of investigators not only easier and efficient, but has helped to reduce concerns about private investigators of the kind expressed by Adrian Roden QC in his 1992 ICAC report[14] about illegally obtained information. It is ironic that the kind of information investigators were seeking in those days (see other expressions of concern about illegal investigations in Australia[15], the United Kingdom[16] and the United States[17]) is now quite easy to obtain on Facebook or other social media sources, an indication of how social media has changed our lifestyles.

The topics for discussion

Social media is a vast topic, so I shall restrict the discussion to the following four areas:

1. What social media is, and how it fits into the information revolution;
2. Legal/illegal use of social media by investigators;
3. The rise of the reputation protection business in the world of social media; and
4. Using social media and other new media to present investigation results.

---

[13] The ICIJ's "Fatal Extraction" report can be viewed at http://projects.icij.org/fatalextraction/s/20. The separate report demonstrating the techniques used to compile this report can be viewed at http://www.icij.org/blog/2015/08/how-we-used-multimedia-tell-fatal-extraction-story.

[14] Adrian Roden QC, "Report on Unauthorised Release of Government Information", Independent Commission Against Corruption, 1992 (2 volumes).

[15] *The Times*, 7 May 1981 reported that a telephone conversation between Prince Charles (holidaying in Australia) and Princess Diana had been intercepted, and that an injunction restraining publication of its contents had been obtained. Mr Ian Sinclair, the Communications Minister, ordered an urgent inquiry, as the tapping had occurred in Australia. The person supplying the transcript, Simon Regan, was an Australian, a former employee of *News of the World* and biographer of Rupert Murdoch. There are many accounts of these events on microfiche (see for example http://archives.chicagotribune.com/1981/05/05/page/9/article/world).

[16] Phone tapping in the United Kingdom was prevalent in the United Kingdom long before the Leveson Inquiry. Books on the history of telephone hacking include Samuel Dash, Richard Schwartz & Robert Knowles, "The Eavesdroppers", 1959; J Courtney, "Electronic eavesdropping, wiretapping and your right to privacy" (1973) 26 Fed. Comm. LJ 1, Patrick Fitzgerald & Mark Leopold, "Stranger on the Line", London 1987 (see the authors' bibliography at pp. 264 – 267).

[17] The most notorious of these prosecutions was Anthony Pellicano, who is currently serving his second sentence for wiretapping. Tabloid journalists have acknowledged using phone tapping; Stuart Goldman describes his initiation into the dark arts in 1988 - 1991, as well as his conviction for hacking offences while carrying out tabloid investigations, in "Spy vs Spy", in *Spy*, Nov- Dec 1995, pp. 34 – 43, https://books.google.ca/books?id=NxR5FFDMZZwC&lpg=PP1&pg=PA32&hl=en#v=onepage&q&f=false.

This means that I will not be covering some of the problem areas of social media use, such as privacy and the impact of surveillance legislation.

Social media arises, of course, from the information technology revolution which has transformed modern communication methods over the past fifty years. The development of the Internet from packet networking in electronic computers in the 1950s to a protocol linking hypertext documents in 1993 (when it communicated only 1% of the world's information!) to its instant domination of the global communication landscape[18] is a little reminiscent of the rise of the machines in the film "The Terminator", so it is appropriate to start this discussion with a story about Arnold Schwarzenegger. It is a story which shows how the work of investigators has changed in the last 10 – 15 years.

Before Total Recall[19]

In early April 2001, actor Arnold Schwarzenegger contacted the celebrated Hollywood private investigator named Anthony ("P.I. to the Stars") Pellicano[20] and his assistant Paul Barresi[21] to offer them an investigation job.

Anthony Pellicano was an old-fashioned private investigator, despite his use of the latest electronic equipment; his speciality was keeping wandering stars such as Michael Jackson out of (rather than in) the news. He and his associate thought they had a pretty good idea of the inquiries Mr Schwarzenegger want them to make, as it was no secret that he was considering running for the 2002 Governor of California election.

---

[18] The date generally given for the Internet's birth is disputed, with some saying it is 2 September 1989 (M Moore "Internet celebrates its 40th birthday, but what date should we be marking?" *the Telegraph* 2 September 2009 (http://www.telegraph.co.uk/technology/6125925/Internet-celebrates-40th-birthday-but-what-date-should-we-be-marking.html).

[19] "Total Recall" is the name of Arnold Schwarzenegger's autobiography, intended by him to "connect the dots" and explain what really happened as opposed to what has been "written about" him: http://www.spiegel.de/international/world/total-recall-schwarzenegger-is-back-a-787753.html.

[20] One of the most prolific phone and computer hacking investigators, Pellicano's acceptance of this work was one of his last jobs before arrest and imprisonment on hacking and tapping charges which will keep him in gaol until 2019. He was already under investigation for his "reputation protection" methods, which included threatening journalists. Police arrested Pellicano for sending a Mafia "message" (a dead fish with a rose in its mouth) to a woman journalist who had threatened to write about some of Pellicano's clients. Police raiding Pellicano's office in 2002 found (and seized) enough explosives to bring down an airliner and "3.868 terabytes of data," the *New York Times* reported during one of his trials, which was "the equivalent of two billion pages of double-spaced text." See *Mail Online*, "Hollywood 'private eye to the stars' faces life in jail for threats and phone tapping" <http://www.dailymail.co.uk/news/article-566745/Hollywood-private-eye-stars-faces-life-jail-threats-phone-tapping.html>.

[21] Mr Barresi, a former adult movies actor who specialised in selling stories to tabloid media brokers, was hired by Pellicano in 1995.

However, Mr Schwarzenegger was to put a proposal to these private detectives which, although unusual at the time, is now one of the biggest areas of work for investigators and "reputation" lawyers today. Mr Schwarzenegger told them:

> "I want you to conduct a top-secret private investigation for me. No expense spared, no questions asked, as fast as you can, and just one copy of your report, for myself only."
>
> "Sure, Mr Schwarzenegger. Who do you want to be investigated?" asked Pellicano, expecting it to be some of the other candidates, or party members opposed to Schwarzenegger's candidacy, or both.
>
> "I want you to investigate myself", replied Schwarzenegger.

So that was what they did. Anthony Pellicano produced a 27-page report less than a week later. It was all there. Schwarzenegger read it all carefully – and made an immediate decision which surprised many people[22]. On April 25 2001 he publicly withdrew from the gubernatorial race, stating that his career and family commitments should take precedence, and that "I have to be selfless at this point."

Far from being selfless, Mr Schwarzenegger had, in fact, performed the first investigative "selfie". He then set about dealing with the reputational issues which could have cost him the race in 2001[23], not announcing his candidature again until 6 August 2003.

This time, the damaging material was a known quantity, and dealt with discreetly. Immediately tagged "the Governator", Schwarzenegger was elected on 7 October 2003, with a 1.3 million vote majority over his opponents (which meant that no run-off vote was required), a position he would hold until he retired from office on 3 January 2011. Only after Mr Schwarzenegger stepped down from office did the stories start to come out – the affairs, the family maid who bore his son[24] - but that is another story, and one which Mr Schwarzenegger, showing his leadership skills in reputation management, is careful to tell in a way which minimises reputation impact[25].

---

[22] "Arnold, Pellicano and Politics", *L A Weekly*, 20 November 2003, http://www.laweekly.com/news/arnold-pellicano-and-politics-2137333.

[23] Some of the methods he used are set out by Saki Knafo, "How did Arnold Schwarzenegger keep his cheating hidden for so long?" *Huffington Post*, 21 May 2011, http://www.huffingtonpost.com.au/2011/05/20/arnold-schwarzenegger_n_864744.html?ir=Australia. Others are set out by Mr Barresi in his 18 August 2008 interview with *Fishbowl: http://www.adweek.com/fishbowlny/investigator-barresi-opens-up-on-hollywood/116345* .

[24] Mr Pellicano has declined to say whether this was known to him at the time of the April 2001 report: Jane Keller, "Anthony Pellicano makes shocking charges about Arnold Schwarzenegger, Michael Jackson", *Hollywood Reporter*, 7 August 2011: http://www.hollywoodreporter.com/thr-esq/anthony-pellicano-makes-shocking-charges-220151.

[25] For a video preview of his book, see https://www.youtube.com/watch?v=7GaDUcMLaeA .

In those innocent days before checking your reputation on Google on a regular basis became a habit for anyone regularly in the news, such a request was considered "bizarre"[26], to quote one of the many of the contemporaneous news reports (this being too good a Hollywood story to keep secret for long).

While Arnold Schwarzenegger was not the first person[27] to check his own reputation by hiring investigators to find out and remove problem areas, his success in putting down the rumours before entering private life, and his continued management of reputation issues, have inspired not only envy but imitation. There is now a whole new industry for reputation management on the Internet in general and social media in particular. While Mr Schwarzenegger may not have invented this new industry, he was the first obvious and public example of how it should be done.

With the rise of social media over the ensuing decade and a half, most members of the community, not just celebrities, now take reputation management seriously; there would be very few experienced social media users who do not regularly check what people are saying about them. This is because the potential for reputation damage in the world of social media is infinitely greater than it was when Mr Schwarzenegger first hired Mr Pellicano. As I set out in more detail below, there is now a vast industry of reputation protection, most of it social media-based, which specialises not only in checking you or your business's reputation, but also in making the bad stories go away. Reputation investigation is big business – and only one of the new investigations businesses, and it is one of a series of profound changes to the work of investigators arising from social media.

What is social media?

Like so many other really useful twentieth-century developments, social media owes its creation and early success to the pornography industry.[28] Social media's security risks[29] largely arise from the interactive nature of social media[30] which is a function of this origin.

---

[26] J R de Szigethy, "Secrets of the Private Eyes", http://www.americanmafia.com/feature_articles_351.html.

[27] For example, *Judicial Watch* reports that President Bill Clinton also asked Pellicano to investigate stories about himself and Gennifer Flowers in 1992: G Rush, J Molloy & S Morgan, " "Ahnold [sic] got Pellicano brief - on self", *New York Daily News*, 21 November 2003, http://www.nydailynews.com/archives/gossip/ahnold-pellicano-article-1.518329.

[28] The pornography industry is now recognised as the market force behind nearly all 20th century communications developments, including camcorders, VHS video, pay-per-view cable and satellite and hotel-based cable: Feona Attwood, "Porn.Com: Making Sense of Online Pornography", New York, Peter Lang, 2010, p. 236. John Arlidge ("The dirty secret that drives new technology: it's porn", *the Guardian*, 3 March 2002) noted that by 2002 there were already 80,000 'adult' and prostitution sites with total profits of more than £1 billion – more than any other e-commerce sector at that time. Many of the first social networks were, however, not pornographic but dating and chat sites, such as IRC (developed in 1988), ICQ and other messaging programmes.

[29] S. Paquette, "Identifying the security risks associated with government use of cloud computing" (2010) *Government Information Quarterly* 245.

[30] Wu He, "A review of social media security risks and mitigation techniques" (2012) 14 *Journal of Systems and Information Technology* 171; S Machkovetch, "Hacked French network exposed its own passwords during TV interview", *Ars Technica*, 11 April 2015.

While social media has been defined by courts in a number of judgments (see, for example, the explanation of Facebook by Blue J in *Von Marburg v Aldred & Anor* [2015] VSC 467 at [9] – [10]), the most helpful explanations are made by the people who use it, such as the actor Stephen Fry,[31] who considers it is a logical extension of the human desire to communicate.

The most common forms of social media are as follows:

1. **Social and information exchange networking sites**, such as Facebook[32], currently the most readily recognisable form of social media and Twitter[33]. Twitter is now so extensively used by academics and lawyers that many courts (such as the Supreme Court and District Courts of New South Wales and the NCAT) have their own Twitter accounts for publication of court information and judgments. Membership is free; this is a feature of almost all social media accounts.
2. **Blogs such as TripAdvisor**[34] which encourage feedback from consumers. These information exchange platforms are probably the most fertile source of reputation damage claims and complaints.
3. **Shared video sources**, the best known of which is YouTube. Although early use was for funny home videos, it now contains extensive legal resources such as court information videos[35] and education courses.
4. **Email and networking sites**, such as Hotmail (set up in 1996) and Yahoo!, which offers web directories as well as the more traditional email services; instant messaging and chat are also offered. At first these were pure email sites, but networking social media sites such as LinkedIn now increasingly promote professional information exchange. Google.com and Gmail now dominate this market.
5. The earliest form of social media on the Internet was for **online sales**. eBay and other online auction or sale websites also provide opportunities for information forums,

[31] https://www.youtube.com/watch?v=ckUpnIc1SF8.
[32] For more information about Facebook, set up in 2004, see footnote 2 above.

[33] Twitter, set up in 2006, has only around 320 million users a month (John McDuling, "Facebook hits the $1 billion mark, leaving Twitter in the dust", *Sydney Morning Herald*, 6 November 2015 (http://www.smh.com.au/business/media-and-marketing/facebook-hits-the-1-billion-mark-leaving-twitter-in-the-dust-20151104-gkr3w8.html). Twitter's use by academics, lawyers, courts and journalists covering court proceedings has, however, given this social media platform significant importance in the legal profession.

[34] There are now entire websites dedicated to reputation protection for restaurants, hotels or other businesses, which receive bad reviews. The site for bad Tripadvisor reviews is at http://tripadvisor-defamation.com/ . Critical reviews are a fertile source of defamation actions.
[35] The South Australian Supreme Court site can be found at https://www.youtube.com/results?search_query=south+australia+supreme+court. The Judicial Commission of NSW site is at https://www.youtube.com/results?search_query=Judicial+Commission+nsw.

blogs, emails and other means of communication through anonymised user names. This includes the ability to use PayPal, the world's first cyberbank. PayPal, first introduced in 1998, was taken over by eBay in 2002 but in July 2015 became a separate entity; early development of online payment system took time because of Internet security issues, which were resolved with the introduction of the security key in 2006.

6. **Chat-based or information sites** like Reddit, photograph and image exchanges such as Instagram, Pinterest, Tumblr and other sites, most of which are iPhone- or iPad-based, as is Skype, a visual telephone link.
7. **Group chat programs and mainstream instant messaging services** such as MSN Messenger. The first, the peer-to-peer file sharing website Napster (where music fans illegally shared music files), was shut down after court proceedings in 2001. While some merely use the programs to chat, others use it for live streaming from concerts, radio podcasts and music downloads. Music downloads are now dominated by Apple's iTunes, launched on April 28, 2003 with just 200,000 songs; by 2011, it was offering 20 million. By 2013 it had sold 25 billion songs.[36]
8. **Collaborative research projects** such as Wikipedia, established in 2001 and originally based on Encyclopaedia Britannica. Wikileaks, the name given to the site containing leaked documents set up by Julian Assange, is unrelated.
9. **Virtual game worlds, social worlds and games[37] and "the dark net"**. Computer consoles, such as PlayStations or Xbox, offer an online community where different users around the world are represented as Avatars. Information can be shared verbally or typed. The dark net needs to be accessed by a Tor browser[38]. A censorship-free world full of anonymous users, the dark net is home not only to criminals but also to whistleblowers, commercial hacking services and online chats and social media sites.

How social media fits into the technological revolution:

[36] http://everystevejobsvideo.com/a-decade-of-itunes-store/.
[37] Geocities, created in 1994, was one of the first social media-style sites.
[38] There are a number of YouTube videos of lectures about social media, and particularly the dark net. One of the safer ones is a TED talk given by Jamie Bartlett at https://www.youtube.com/watch?v=pzN4WGPC4kc.

"Social media" needs to be seen in context as one of a series of interrelated technological innovations that will fundamentally alter the workplace generally, and not just how investigations are carried out. These are:

- Mobile computing and wireless technology.[39]
- Interconnectivity, notably 'the Internet of Things'[40] and cloud computing.
- "Big data" analysis (e.g. the use of "predictive coding"[41] in big data management).
- Electronic records management systems ("ERMS") for retention of electronically stored information ("ESI").
- Social media and its interaction with these new forms of technology.[42]

The rapid changes to document creation and management resulting from all these innovations are interconnected. Social media is only part of the picture.

2. Using investigative material in court

Until the advent of social media, CCTV and computerised public records, investigators' means of obtaining information about claims were limited, no matter how worthwhile or urgent the inquiry was. For example, investigators of claims for personal injury damage had to rely upon surreptitious film of the plaintiff, discreet inquiries of the neighbours and limited public records such as ASIC searches. Even searching the target's rubbish bin could be a risky proposition[43]. A private inquiry agent who attends a private meeting on behalf of a client runs the risk not only of unpleasantness on discovery but also unpleasant news coverage of his activities, as insurance fraud investigator David Seedsman found when he attended an anti-poker machine meeting in a country town[44].

[39] Many courts have committees to deal with the impact of wireless technology and social media on courts. One of many in the United States is the Arizona Judicial Branch, established on 7 March 2012 to advise the court on rule changes and ethical issues arising from social media and Internet use, and to report to the Judicial Council. These judges' insightful report (and arresting front page artwork) can be found at http://www.azcourts.gov/Portals/74/WIRE/FinalWirelessReportRED.pdf.

[40] Gregory J Millman explains this in "Cyber Cavalry rides to the rescue of the Internet of Things", *Wall Street Journal*, May 5, 2014. Transmissions from one device to another can occur involuntarily, but fears that electronic equipment spies on its users (G Adams, "Is your TV spying on YOU?" *Daily Mail*, 26 November 2013) appear unfounded: *Download this Show*, Australian Broadcasting Corporation, 14 February 2015.

[41] Predictive coding enables identification of relevant documents in large e-discoveries; see S Nance-Nash, "Predictive coding and emerging e-discovery rules", *Corporate Secretary*, 14 August 2013.

[42] I have based this on a similar list given by Norman H Meyer, Jr in "Social Media and the Courts: Innovative Tools or Dangerous Fad? A Practical Guide for Court Administrators", (2014) 6(1) *International Journal for Court Administration*, p. 2 ("Norman Meyer").

[43] The most celebrated bin forager, "Benji the Bin Man", supplied documents taken from garbage bins to journalists in England during the years of the phone hacking scandal, but was convicted several times for these activities: Kevin Maguire, "Muckraker who feeds off bins of the famous", *the Guardian*, 27 July 2000, http://www.theguardian.com/uk/2000/jul/27/labour.politics.

[44] K Needham, "Intimidation claims after anti-poker machine meeting", *Sydney Morning Herald*, 8 November 2011 (http://www.smh.com.au/nsw/intimidation-claims-after-anti-poker-machine-meeting-20151105-gkry2d). If, as this article appeared to suggest, he was intending to emulate the private investigator in *Bennette v Cohen*

When this kind of material was obtained, the next question was how to use it in court. Where surveillance film or similar material was being used, it generally had to be provided to the opponent prior to the hearing in accordance with procedural rules such as Uniform Civil Procedure Rules r 31.10. The so-called *Markus* privilege from production of documents or evidence was developed as an exception to production prior to trial, based on the court's recognition that compliance with court orders for production of evidence or documents carries the risk that the opposing party may tailor the evidence based on that discovery: *Halpin v Lumley General Insurance Ltd* (2009) 78 NSWLR 265; *Hammoud Brothers Pty Ltd v Insurance Australia Ltd* [2004] NSWCA 366 at [10].

The *Markus* privilege may apply to a wide range of evidence and documents, ranging from Anton Piller orders (*Ho v Fordyce (Ex parte)* [2012] NSWSC 1404) to inspection of documents produced on discovery (*Morton v Colonial Mutual Life Insurance Society Ltd* [2013] FCA 681). It can also apply documents sought under subpoena: *Marsden v Amalgamated Television Services Pty Ltd* [1999] NSWSC 428 (referred to in *Halpin v Lumley General Insurance Ltd*, *supra*). However, the application may not succeed and, even if it does, the surprise factor may be lost if the opposing party is put on notice of it.

However, life is much easier for investigators now, thanks to the advent of social media. First of all, material is much easier to collect. A party under cross-examination about ongoing disabilities can be shown, without any notice, extracts from a social media record such as Facebook showing fast cars and fitness activities, as occurred in *Saleh v Faddoul* [2015] NSWDC 184 at [82] and in *Ballandis v Swebbs* [2014] QDC 129 at [29] – [30], to cite two recent examples. Tender of social media (and service of recalcitrant or missing parties by sending the relevant court documents to their social media account) are such a staple of Family Court proceedings that it is no longer necessary to cite case examples.

Unlike the bad old days when investigators resorted to methods of the kinds outlined in the ICAC *Report on Unauthorised Release of Government Information*,[45] social media is also an invaluable way of finding out about people and activities. For example, Mr Seedsman does not need to go to a meeting to find out who is opposing his client's application to install poker machines, and what they are saying; he can easily find out who is opposed to poker machines in Casula by looking on the Facebook page of the Casula Community Group for

---

(2007) Aust Torts Reports 81-897 at [201]; [2009] NSWCA 60 at [119] – [121], it will be interesting to see if judges today take the same condign view as the trial judge did on surreptitious recordings (at [201]):

> "Nor, in my opinion, was the use of a private investigator secretly to record what occurred at the meeting indicative of some form of wrongful conduct or manipulation of the system. The position may have been otherwise if the plaintiff, or his identified representative, had turned up at the meeting seeking to interrupt it, or to threaten or intimidate those proposing to attend it. Although there may conceivably be cases where the means, by which a plaintiff comes to be possessed of the detail of what a defendant has published, assume importance, the present is not such a case. I consider it to be a neutral factor."

[45] Independent Commission Against Corruption, 1992 (2 vols).

Responsible Planning Inc[46] (their logo is "No pubs and pokies in Casula"), or on Twitter for comments.[47] This is quite legitimate, as these are publicly available documents.

Secondly, when considering the admissibility of such information in court, social media pages are being tendered without any significant challenge. After all, how can a party be forced to discover or give early disclosure to the opposing party the photographs and posts gleaned from his/her own Facebook pages? The few cases reporting that social media tenders have been made simply note that the evidence has been tendered without setting out any basis for objection. Social media entries have been successfully used in personal injury cases as appellate level: *Frost v Kourouche* (2014) 86 NSWLR 214 (see also *Munday v Court* (2013) 65 MVR 251).

Social media and criminal investigations

While current views are existing legislation will suffice,[48] the investigator will be faced with novel problems, including:

(a) Social media will need to be monitored for adverse pre-trial publicity[49], including publicity during the hearing such as tweeting from court.[50] This would include monitoring for possible breaches of suppression orders.[51]

(b) Where identification is an issue, crime investigators will have to be particularly vigilant to guard against social media photographs contaminating evidence, as Peek J pointed out in *Strauss v Police* [2013]115 SASR 90 at [12] – [37] ("Part 2: Identification evidence in the age of Facebook"); see also *R v Crawford* [2015] SASCFC 112

(c) Most if not all jurors use social media, and the days when a Skaf direction would discourage this are long gone.[52] Constant monitoring of social media and the use of suppression or other orders to prevent the publication of prejudicial or confidential material will be necessary.

---

[46] https://www.facebook.com/Casula-Community-Group-For-Responsible-Planning-Inc-1455221998055790/?fref=ts.

[47] https://twitter.com/search?q=Casula%20pokies&src=typd.

[48] House of Lords Select Committee on Investigations, "Social Media and Criminal Investigations", 1st Report of Session, 2014 – 5, http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/37.pdf.

[49] "Pre-Trial Publicity, Social Media and the 'Fair Trial'" (2013) 33 *Qld Lawyer* 38.

[50] In November 2011, Magistrate Peter Mealy complained that tweeting "will be contempt if it does occur from this court" after discovering a freelance journalist from *Crikey* sending live tweets from the courtroom where a committal was under way; taken from P Akerman, "Magistrate hearing evidence against Simon Artz bans Twitter from court", *the Australian*, 4 November 2011.

[51] David Barnfield, "Effectiveness of Suppression Orders in the Face of Social Media" (2011) 33(4) *LSB* 16; B Fitzgerald and C Foong, "Suppression orders after *Fairfax v Ibrahim: Implications for Internet Publications*" (2013) 37 *Aust Bar Rev* 175.

[52] M Krawitz, "Guilty as Tweeted", University of Western Australia Faculty of Law Research Paper 2012. For a commentary from the United States, see Meghan Dunn, "Jurors' Use of Social Media During Trials and Deliberations", Federal Judicial Center, 2011; her survey of 508 US judges also sets out sample jury instructions some participating judges have given in court.

However, social media can be, and has been, a highly successful tool in criminal proceedings. Police use social media widely for a variety of reasons, including public requests for witnesses to crimes or motor vehicle accidents. This has been recognised by the court as a significant investigation tool: *R v Crawford* [2015] SASCFC 112 at [57].

Members of the public can also launch their own social media inquiries if they are seeking assistance after a crime has been committed. A good (though tragic) example is the quick-thinking Mr Tom Meagher who, when his wife did not come home from a social function, not only contacted police but asked his ABC colleagues to use Twitter and other social media to find her. A Facebook page, "Help us find Jill Meagher", was set up the day after her disappearance and attracted 100,000 "likes". The widespread publicity caused many people to make searches, and check CCTV footage from cameras outside their shops or premises. This was what led to the CCTV footage of the offender being located so quickly (three days after her disappearance). That CCTV footage was crucial evidence. Additionally, three more rape victims came forward as a result of the publicity[53].

The ease with which such evidence may be tendered in criminal proceedings is what makes social media evidence so useful. Tender of phone SMS and social media records in criminal trials is now almost as common as CCTV, leading some police to suggest that in the 21st century it will no longer be possible to commit the perfect crime because the technological footprint we leave (including social media) makes discovery of evidence so much easier[54].

However, the Meagher murder investigation also illustrated some of the drawbacks to social media use where criminal proceedings are on foot. The story continued to dominate social media for weeks, with around 12 million timelines on Twitter referring to it, according to the Jill Meagher murder Wikipedia website. After the arrest of the person ultimately convicted of the murder, Victorian police sought the removal of Facebook pages, concerned that the potential pollution of identification evidence would cause problems at the trial, as well as by hostility towards the accused. Facebook refused,[55] and the police had to make a plea from their own Facebook account for Facebook users to stop.[56]

---

[53] Wikipedia, "Death of Jill Meagher", https://en.wikipedia.org/wiki/Death_of_Jill_Meagher.

[54] See the review of social media history in https://www.youtube.com/watch?v=uquRzrcwA18&list=PLVVx5SlGAsizCNsp887d1qpxzJOu_QmmK&index=6.

[55] Facebook initially refused to remove the Meagher page: ABC News: "Facebook refuses to remove the Meagher page", 1 October 2012 (http://www.abc.net.au/news/2012-10-01/facebook-refuses-to-remove-meagher-page/4289262).

[56] Adrian Lowe, "'Trial by social media' worry in Meagher case", *the Age*, 28 September 2012 (http://www.theage.com.au/technology/technology-news/trial-by-social-media-worry-in-meagher-case-20120928-26pe4.html).

Where a person has been publicly identified on social media as being guilty, this may lead to claims that the jury pool's mind is poisoned. The television personality Robert Hughes has recently argued he had not received a fair trial because of prejudicial publicity on social media websites.[57] There are, however, two points to note. The first is that such claims have been made in relation to more traditional media sources (notably television), and the second is that they have been, with one exception, unsuccessful where a stay of proceedings has been sought. Australian courts have taken a robust view of prejudicial publicity, *Tuckiar v The King* (1934) 52 CLR 335 being the exception which proves the rule.[58] This view of *Tuckiar* was recently affirmed in *R v Lloyd Patrick Rayney (No 3)* [2014] WADC 117, where widespread vilification on social media was insufficient basis for a permanent stay.

The most common request an investigator will receive, whether the case is civil or criminal, is to find and stop the publications. As the cases on this topic demonstrate, this is not always easy. This brings me to the third topic for discussion: investigation of reputation damage from social media and Internet sites.

3. The reputation game: *Duffy v Google Inc* [2015] SASC 170; *Bleyer v Google Inc* [2014] NSWSC 497

As I noted at the commencement of this discussion paper, there are now vast business empires offering to vacuum the Internet to remove your client's own posts, search for quotes traducing your client's reputation and/or conduct inquiries into persons targeting persons cybertrolling or harassing your client. The principal reason for this is the lively (and often defamatory) exchange of information and opinions on social media, chat forums and blog sites, which ranges from giving ratings to everyone from dentists to dog groomers to warning about bad tradesmen.

Where an Internet search reveals a hostile review, or an attack by a business rival, what should a party do? There are two possible avenues: court proceedings and non-litigious negotiations. In the two cases for discussion, the plaintiffs (Dr Duffy and Mr Bleyer) chose to go to court. They were targets of online vilification, rather than specific social media attacks, but the principles are the same.

Dr Duffy was the subject of six articles on the Ripoff Report website between 2007 and 2009. She was able to persuade Google to take down the Ripoff Report website entries, but not the links to these documents on other websites or social media. Like Dr Duffy, Mr Bleyer was

[57] Stephanie Gardiner, "Hey Dad! actor Robert Hughes subject of 'poisonous and vile' social media: appeal", *Sydney Morning Herald*, 28 September 2015 (http://www.smh.com.au/nsw/robert-hughes-the-subject-of-poisonous-and-vile-social-media-appeal-hears-20150928-gjwa1z.html).

[58] For a discussion of cases since *Tuckiar v The King* see Craig Burgess, "Prejudicial Publicity: will it *ever* result in a permanent stay of proceedings?" (2009) 28 Tas L Rev 63. As Mr Burgess notes in his conclusion, the Internet and what he calls the social media "revolution" mean that the public today receives a great deal more information than was the case in 1934; only a "truly exceptional" case would warrant a permanent stay of criminal proceedings.

the subject of attacks which came up as "snippets" in the Google search engine, although he was much more successful in having them removed promptly.

Both commenced proceedings against Google Inc in relation to the lingering traces of the libels. Dr Duffy was successful (although the judgment has been appealed), and Mr Bleyer was not. Both cases illustrate the perils of taking anyone, including the search engine, to court. Here are some of the problems they encountered.

Proving publication:

Where a publication damaging to a person or business is made on the Internet, the courts do not automatically accept that somebody must have read it. Material available on the worldwide web is not published simply by some "unilateral act on the part of the publisher" (*Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575 at 600 ("Dow Jones") in uploading the material. Publication is a "bilateral act"; there must be particulars provided of the downloading of an article by a person who was able to understand it in the language in which it appeared (or alternatively, used the translation button).[59] That person has to be a genuine third person, not someone asked to look at the material by the plaintiff (*Duffy v Google Inc* at [281] – [283]).

Both Mr Bleyer and Dr Duffy had trouble proving publication to third parties. In Mr Bleyer's case, this was one of the reasons for his proceedings being dismissed on the "*Jameel* principle" (*Dow Jones & Co Inc v Jameel* [2005] EWCA Civ 75) basis; the extremely limited publication (effectively only one person) was simply insufficient to warrant his being permitted to go on with the claim.

In *Duffy v Google Inc*, Dr Duffy relied on evidence of readership from three sources. The first was a Mr Trkjula, who had himself instituted a series of actions against Google. His evidence was that he read about Dr Duffy's court proceedings in *the Age* and carried out searches. His evidence was so inconsistent that Blue J did not accept it (at [293]). Secondly, Dr Duffy called witnesses from the Department of Health. One of them, Mr Shearer, could not say if he used the Google search engine or not (at [295]) and the others did not use Google for their searches (at [296]). The third was a Ms Palumbo, who carried out the search independently, but only after Dr Duffy raised the problem with her, which Google claimed did not amount to an actionable publication (at [281]).

If a plaintiff shows the matter complained of to someone, does that amount to publication to a third party? Google argued that it could not. Blue J noted this problem at [281] – [283]:

> "[281] Google contends that "publication" must be to a person other than someone "in the plaintiff's camp" and must be to a person who has given the imputations a measure of credence rather than merely to a person such as a friend or colleague who has viewed the material at the plaintiff's request and not attached any weight to it. Google does not contend

[59] The communication of material on the Internet in non-readable form, such as computer code, will not ordinarily constitute publication: *Collins*, "The Law of Defamation and the Internet", *Oxford University Press*, 3rd ed., 2011 at 5.04.

> that Ms Palumbo fell within the plaintiff's camp for this purpose when she undertook the 2010 searches but contends that she did so when she undertook the 2012 and 2015 searches. The only search in respect of which this is a live issue is the 2012 search producing the Autocomplete alternative search term "janice duffy psychic stalker".
>
> [282] I reject Google's contention. It is well established that publication is complete and the cause of action in defamation is good even if the publishee does not believe the imputation or give it any credence. Google's proposition of law summarised in the previous paragraph was rejected by the English Court of Appeal in *Dow Jones & Co Inc v Jameel*. The doctrine developed and applied by the Court of Appeal in that case, namely that it may be an abuse of process to sue for defamation when the publication has been minimal and caused no significant damage to the claimant's reputation such that the expense of an action is disproportionate to the available remedy, is inconsistent with Google's proposition of law."
>
> [283] I accept (without deciding) that there might not be an actionable publication if a plaintiff instigates a friend to access from a website defamatory matter solely for the purpose of the plaintiff relying on it as publication to give rise to a cause of action. However, while Ms Palumbo made her search in 2012 following and as a result of Dr Duffy telling her that the defamatory material was still on the internet, she nevertheless made that search of her own volition and it was not instigated by Dr Duffy." [citations omitted]

Ms Palumbo only got over the hurdle because of this factual finding. She was the only individual who could be established to have read the download at the relevant time. Although the trial judge went on to make findings that "persons unknown" downloaded the material because of clicks on the website, the very limited publication will create real problems on damages issues (assuming this finding survives appeal). What Dr Duffy's and Mr Bleyer's cases show is that before going to court, there should be sufficient evidence of publication to make the court proceedings viable.

Finding (and stopping) the defendant

The real solution is, in my view, not going to court for damages, but stopping the anonymous poster, and this is where the Internet investigator comes in. The most common problems for investigation are:

- Identifying the anonymous defendant.
- Finding a defendant with assets in the jurisdiction – failure to do so was part of the reason why Mr Bleyer's action was struck out.
- Stopping the defendant from continuing to post elsewhere

Finding the anonymous poster

Many, if not most, social media posts are anonymous. Why is social media anonymity such a problem? The July 2014 House of Lords[60] report on the adequacy of criminal law to deal with social media offences commented:

> "50. The internet readily facilitates its users doing so anonymously. Although it is possible to identify (including retrospectively) which computer in the world was used to post a statement (because each computer has a unique "internet protocol address"), it is not necessarily possible to identify who used that computer to do so.
> 51. This is in part because many website operators facilitate the anonymous use of their service. There is no consistent attitude taken by website operators: some require the use of real names (Facebook, although they do not actively confirm users' identities); some allow anonymity but challenge impersonation (Twitter); others allow absolute anonymity. Google+ abandoned its real name policy and apologised for having tried to introduce one."[61]

Dr Duffy and Mr Bleyer really brought proceedings against Google because individual Facebook posters were likely to be men of straw. The problem is that there can be no liability until the defamatory post is brought to their attention; if it is removed immediately, as occurred in Mr Bleyer's case, the plaintiff may end up with no action at all. Bringing proceedings against the Facebook administrator or the leader of the organisation whose publications cause the problems is just as difficult, although for other reasons: *Von Marburg v Aldred & Anor* [2015] VSC 467.

Early retention of documents

Dr Duffy also sought to establish publication by "persons unknown" (*Duffy v Google Inc* at [297] – [345]). This was difficult because Google had not retained any data showing the number of searches for the plaintiff before August 2013. Blue J noted at [309]:

> "Google has not retained any data showing the number of searches on the Google Australian website for "Dr Janice Duffy" and "Janice Duffy" before August 2013. That data would have been available for at least the 12 months ending in March 2011 if Google had chosen to retain it upon being served with the summons in the action."

However, it is open to a plaintiff to serve, along with the pleading which initiates proceedings, a request for retention of material. This is what Dr Duffy should have done, and it is an essential part of any investigation of the facts in cases such as these.

Removing the posts

Reputation protection businesses such as Regain your Name[62] offer a range of services including:

- Removing insulting or embarrassing entries on Wikipedia;

[60] House of Lords Select Committee on Communications' 1st Report of Session (29 July 2014).
[61] Loc. cit., at pp. 15 – 16.
[62] Their site may be seen at http://regainyourname.com/. There are also Twitter and Facebook accounts for this organisation.

- Deleting Google searches and snippets;
- Removing and blocking cyberbullying and trolling messages on social media;
- Action to remove false or defamatory "reviews" on sites such as Tripadvisor and Trivago.

Removing all the posts can be a problem, even for the honest defendant. For example, I heard a case in 2010 where Nationwide News Pty Ltd had been ordered to remove posts about a child the subject of Children's Court proceedings. They really tried hard, but the story had gone viral. Some of the difficulties they had are set out by me in *XX v Nationwide News Pty Ltd* [2010] NSWDC 147.

In those proceedings, an application for indemnity costs was made on the basis, inter alia, that articles about this child still appeared on the Internet despite programs for their removal. Nationwide News Pty Ltd explained the continued appearances of these articles as being because of a changeover from "Vignette" to "Fatwire"[63] content management system programmes (at [36]). However, their inability to remove all the posts exposed them to an indemnity costs order.

Are court proceedings worth the costs and time?

Court proceedings against search engine may be appropriate where what is complained about are "snippets", or search engine results, where the search engine has been asked to remove the material.

In the case of Mr Bleyer, Google's prompt action had fatal consequences for his claim, in that it meant he could only identify one person who read it after the request for Google to remove the posts. Mr Bleyer abandoned the proceedings after his claim was struck out on proportionality grounds, but it is worth noting that the concept of proportionality remains untested on appeal, as the Court of Appeal refrained from dealing with it in *Ghosh v Ninemsn Pty Ltd* [2015] NSWCA 334, preferring instead to dismiss the appeal on the more traditional ground that the claim was an abuse of process[64].

While Dr Duffy may be successful on appeal, and the courts in Australia have not yet endorsed the principle of proportionality which cost Mr Bleyer his case, the merits of claims

[63] Vignette and Fatwire were content management systems in use at the time: http://www.cmswire.com/cms/web-cms/fatwire-swoops-on-interwoven-and-vignette-customers-004837.php. Fatwire has since been acquired by Oracle: http://www.oracle.com/us/corporate/acquisitions/fatwire/index.html.

[64] A similar reluctance to adopt the "*Jameel* principle" (*Dow Jones & Co Inc v Jameel* [2005] EWCA Civ 75) may be seen in the Canadian courts. In *Frank v Legate* [2015] ONSC 631 the Court dismissed the claim as an abuse of process without referring to the *Jameel* principle. *Jameel* was relied upon, without success, in *Goldhar v Haaretz.com et al* [2015] ONSC 1128, and noted as being foreign jurisprudence in *Bou Malhab* c. *Diffusion Métromédia CMR inc. et al.*[2011] CSC 9 at [20] per Deschamps J, cited most recently in *3834310 Canada inc. c. Pétrolia inc.* [2011] QCCS 4014 at [20]. Actions for defamation have, however, been struck out as an abuse of process on more general principles; for a recent discussion, see *Daniels Midtown Corporation v Mariai* [2015] ONSC 6568 (application refused)

such as this are hard to ascertain. Embarrassing photographs or bullying posts can be more easily (and much more cheaply) dealt with outside the parameters of court proceedings.

A good investigator should also be able to advise clients about internal and external social media policies and how to deal with crises on social media without going to court. While technically a court could order the removal of such posts, this is never easy, no matter how flagrant the language, because of free speech concerns. Even if the court proceedings are successful, the cost is enormous and the result may be Pyrrhic, as Seafolly found in *Madden v Seafolly Pty Ltd* [2012] 297 ALR 337; [2014] FCAFC 30.The problem for Seafolly was that they had not actually suffered any loss, and had to content themselves with a nominal award of $25,000, whereas their response to the business rival whom they had sued was held to be defamatory and damages were awarded against them for that publication.

4. Use of social media to prepare and present investigative reports

As I noted at the commencement of this discussion paper, some enterprising investigators are using social media to ascertain troop movements[65] or Australian companies' environmental and social footprints in Africa.[66] For investigative journalists of the future, social media use is an exciting area; for example, Kate McClymont's tweets from the ICAC inquiries over the past two years have been front page news and have won her awards.

In "Fatal Extraction", the story of Australian mining's vast but rarely-examined social and environmental footprint in Africa, ICIJ not only used social media sources to compile report which is striking for its presentation methods, but prepared a separate report setting out how they did it.[67] This technique-sharing approach is common to many of these investigative sites (e.g. Bellingcat).

Some investigator websites have noted this trend. For example, Benjamin Wright, writing for DFI News[68], points out that investigators can make their courtroom evidence more attractive by using new technology such as screencast video recording technology.

Social media is useful for visually-based investigations by amateurs, such as the exposé of a Chinese official's corruption by posting multiple photographs of all his expensive

[65] This is one of a series of Bellingcat's "how to" YouTube discussions: https://www.youtube.com/watch?v=flCqN8_0cX4 . This is called "geolocating": https://www.youtube.com/watch?v=7bxvEWZgCM8.
[66] http://projects.icij.org/fatalextraction/s/20.
[67] http://www.icij.org/blog/2015/08/how-we-used-multimedia-tell-fatal-extraction-story
[68] "Social Media and the Changing Role of Investigators", Digital Forensic Investigator website, 20 December 2012 (http://www.forensicmag.com/articles/2012/12/social-media-and-changing-role-investigators).

wristwatches[69]. The same technique was used to post photographs of the $600,000 watch worn by Vladimir Putin's press secretary, Dmitry Peskov.[70]

The ease of use of social media for investigation may, as a result, be a two-edged sword. Just as the usefulness of Twitter for journalists in the courtroom has led to an influx of "citizen journalists", a new breed of "citizen investigators" has sprung up. Armed only with a mobile phone, any member of the public can investigate a person or issue and publicise those results on social media. The success of social media campaigns to expose Jimmy Savile and a series of British and Irish children's homes;[71] Catherine Corless, the Irish amateur historian who posted groundbreaking research into infant deaths in children's homes on her Facebook Page[72] and the social media campaign for an inquiry into the 1987 murder of a private investigator named Daniel Morgan[73] are three telling examples of this trend.

"We can remember it for you wholesale"[74]

Electronic publication fundamentally changes the nature of information retention, which is universal, permanent and vast: "God forgives and forgets, but the Internet never does."[75] Social media does not want us to have the right to be forgotten,[76] which has advantages for investigators as well as advertisers, as social media permits everyone to leave their personal imprint on the public memory.

---

[69] Jonathan Kaiman, "China's 'Brother Wristwatch' Jailed 14 years for corruption", *the Guardian*, 5 September 2013 (http://www.theguardian.com/world/2013/sep/05/china-brother-wristwatch-yang-dacai-sentenced).

[70] This is the subject of a Bellingcat report: https://www.bellingcat.com/category/resources/case-studies/

[71] "Notes on a Scandal: the Jimmy Savile Case is All Too Familiar", *The Conversation*, December 17, 2013 (http://theconversation.com/notes-on-a-scandal-the-jimmy-savile-case-is-all-too-familiar-20379).

[72] Amelia Gentleman, "The mother behind the Galway children's mass grave: I want to know who's down there", *the Guardian*, 14 June 2014 (http://www.theguardian.com/world/2014/jun/13/mother-behind-galway-childrens-mass-grave-story).

[73] There is so much material on social media that Wikipedia is the best source: https://en.wikipedia.org/wiki/Daniel_Morgan_(private_investigator) . To date there have been five police inquiries and there is an independent committee of inquiry which has not yet completed its hearings. The police have acknowledged that police corruption played a role in the cover-up of the murder of the investigator. Charges were dropped against the chief suspect, his partner, and three other remaining accused in 2011. For recent commentary on the information being considered by the current inquiry see Peter Jukes, "Miskiw confirms: News of The World subverted murder inquiry on behalf of murder suspects", *Byline*,6 November 2015 (https://www.byline.com/column/2/article/571).

[74] This is the title of the Philip K Dick short story upon which the film "Total Recall" was based.

[75] Viviane Reding, Vice-President of the European Commission, European Data Protection and Privacy Conference, 30 November 2010, http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm .

[76] Samuel Gibbs, "Facebook questions use of 'right to be forgotten ruling'", *the Guardian*, 8 July 2015 (http://www.theguardian.com/technology/2015/jul/07/facebook-questions-use-of-right-to-be-forgotten-ruling).

This is why, as LexisNexis point out in their useful monograph "One Step Ahead: How Social Media is Changing the Face of Investigations",[77] social media is changing every aspect of the work of the investigator. Law enforcement's use of social media to track information previously not available, such as riot control and terrorism activities, was one of the first recognitions of these possibilities, and integrating social media data into intelligence analysis is now commonplace. The same advantages are there for professional investigators, whether the subject matter is financial fraud, surveillance of an injured person for court proceedings, or document examination.

The presentation methods available from social media and information technology not only help the investigator to carry out his inquiries, but also to present the data collected, whether to the courtroom or to the client, in a concise and comprehensive picture. For example, I could live-stream this presentation on Twitter's Periscope to anyone, anywhere in the world.

In the future, as the lines between social media and Internet communication become increasingly blurred, the whole nature of communication will change. No doubt the role of the investigator will change as well. The whole concept of privacy of information is shifting, and the way in which we interpret and investigate information will change with it. However, while the manner of human discourse will change, there will always be cheating spouses, missing money and crooked officials, so investigators (unlike, perhaps, judges, or even lawyers) will always be in business.

[77] This article can be found at http://www.lexisnexis.com/risk/downloads/assets/one-step-ahead.pdf.