Reputation in the digital age: how to combat online reputational risks

Reputation is of universal importance. However, the stakes are particularly high for high-net-worth (HNW) individuals and families, who often have a higher public profile and therefore have more at stake. Further, should an issue arise, those individuals will often be deemed of heightened newsworthiness in light of their standing, success and wealth.

This chapter addresses common problems encountered online and the ways in which these can be addressed, as well as proactive steps which can be taken in privacy planning and to manage digital footprints before a crisis arises.

As the authors are solicitors qualified in England and Wales, the content of this chapter draws largely from the position as it is under domestic law in that jurisdiction. However, it is hoped that this chapter will serve as a helpful starting point in considering reputational challenges online, wherever the relevant parties are based.

> “ The speed with which information can spread online is unparalleled. Seeking advice before a crisis arises means that a plan of action can be put in place in advance and decisions need not be made under intense time pressure.

The nature of reputational risks in the digital age

Reputational risks are heightened in the digital age due to the ease and speed with which information can be disseminated. Further, the 24-hour news cycle and a news marketplace where the competition is continually expanding have increased the pressure on news outlets to produce more content, more quickly. Whereas in the past, at many news publishers all content would be run past the legal department, this is now no longer the norm.

Further, increasingly, news is distributed via alternative channels such as WhatsApp groups and online forums which are not subject to the same – if any – level of assessment prior to publication. This has undoubtedly contributed to


Perveen Hill
Senior Associate | London
perveen.hill@withersworldwide.com


Jo Sanders
Partner | London
jo.sanders@withersworldwide.com


Caroline Thompson
Special Counsel | London
caroline.thompson@withersworldwide.com

an environment in which 'fake news' can flourish. Deepfake technology also poses significant challenges and has facilitated the spread of falsehoods online via unnervingly realistic and credible videos and images.

While to a large extent it is still an individual's conduct which will affect how others perceive them, the Internet provides a separate platform on which an individual's reputation can be made or broken – often at some remove from the individual themselves.

Common considerations when dealing with online content

Before considering specific categories of problematic online content, it is worth briefly addressing four common issues of universal application to reputational issues which arise online:

- the importance of acting swiftly;
- where to seek advice when a reputational issue arises online;
- the preservation of online content; and
- dealing with anonymity online.

Responding swiftly to online reputational threats

The speed with which information can spread online is unparalleled. Seeking advice before a crisis arises means that a plan of action can be put in place in advance and decisions need not be made under intense time pressure. Further, it may be helpful to be able to consult with a range of advisers, including communications specialists, and other key stakeholders in advance of any publication or disclosure.

Once harmful content has been released, prevarication can result in attempts to remove or counter the harmful content becoming more challenging and costly. Undue delay can also complicate or even preclude pursuit of legal action against the perpetrators.

Seeking advice when problematic information is shared globally

The next important consideration is where to seek legal advice. In some instances, there will be a clear

answer. However, if the individual affected by the online activity has links to various jurisdictions and a global reputation, the decision-making process may be more byzantine.

In contrast to the borderless nature of the Internet, our judicial systems remain tightly tied to distinct jurisdictions or regions. This can present additional challenges in seeking remedies that provide adequate redress for harm which may be being caused internationally across various jurisdictions.

Consideration should be given to the following non-exhaustive factors:

- the jurisdiction in which the author/publisher of the (anticipated) content is based;
- the jurisdiction in which the online platform or service provider that hosts or distributes the (anticipated) content is based;
- the jurisdiction(s) in which the online audience of the (anticipated) content is based;
- the jurisdiction(s) in which interested media parties or other stakeholders that may report or comment on the (anticipated) online content are based;
- the jurisdiction(s) with which the prospective claimant has personal or professional ties – (ie, in which jurisdictions does the prospective claimant have a reputation to protect?); and
- the standing of the court system in any relevant jurisdiction(s) – is there, for example, a risk that if legal action had to be taken and was ultimately successful, the validity of any judgment could be brought into question due to widespread allegations of corruption within that judicial system?

The approach of different courts can be fairly stark and therefore the same complaint may be treated very differently by different authorities as regards:

- the nature and validity of the legal complaint;
- the appropriate dispute resolution procedure;
- available remedies;
- means of enforcement; and
- costs.

It may be appropriate to take advice in a number of jurisdictions in order to consider in which jurisdiction the prospective claimant would have the best prospects of success not only in establishing their legal case, but also in obtaining and enforcing remedies of the greatest benefit. Another factor in selecting the jurisdiction in which to ground any complaint may be the efficiency of the courts and the likely timeframe for resolving any proceedings that are commenced. There may also be additional relevant considerations such as the differing approaches of different courts to anonymising proceedings or holding hearings in private; as well as the costs of taking action in different jurisdictions.

Often it is not necessary to commence formal court proceedings in order to obtain the remedies that a claimant requires. The majority of claims are resolved out of court and at a pre-action stage. In some cases, there could be a reputational risk attached to initiating or threatening legal action – even where the claimant has a legitimate complaint – if this could be perceived as a disproportionate reaction or where publication is warranted in the public interest. This underlines the importance of seeking advice and setting a clear and considered strategy in response to a reputational crisis at the earliest opportunity.

Preserving content

When faced with harmful or false information posted online, the immediate reaction of many individuals and corporates, as well as their advisers, may be to seek immediate deletion of the material. However, it is extremely important – particularly when there is any possibility of legal proceedings or a report to the police – that relevant information and evidence be preserved prior to deletion. Digital specialists can run and analyse interaction and engagement with social media posts and other online activity to facilitate the gathering and presentation of evidence in support of a legal claim.

Dealing with threats posed by anonymous persons online

There are additional logistical and strategic challenges where the unwelcome activity emanates from an anonymous individual or group online. However, anonymity does not preclude obtaining effective legal remedies. There may be a number of avenues for obtaining information as regards the identity and location of an anonymous prospective defendant, including via a third-party disclosure order or a request to the online platform on which the material is hosted. Alternatively, the courts may be prepared to grant injunctive relief against 'persons unknown' which can be used to ensure that third parties, such as website hosts or internet service providers, assist in the removal of unlawful content.

Online libel

Is it libellous?

Defamation (of which libel is the subset of statements made in permanent form, including online) is often misused to mean anything that is negative or derogatory. In fact, it has highly technical requirements. In English law, it is a statement that tends to lower a person in the estimation of others and it must cause serious harm to that person's reputation. It must also be made to a third party – it is not defamatory to be offensive directly to that person (though that might form part of harassment).

When deciding whether something posted on social media is libellous, or indeed what a statement means, the test is what an ordinary social media user would think.[1] This involves considering how tweets or posts

1 *Stocker v Stocker* [2019] UKSC 17.

are made and read. Context is everything. This can be complex when considering reply tweets or posts which link or refer to other content.

Can it be defended?

Even if a statement is defamatory, it might still be lawful if it is true, an opinion or on a subject that is of public interest. There is special protection for some speech, including reports of Parliament and courts.

Legal remedies

A court cannot make someone apologise for what they have said or force them to retract it. However, a judicial finding that an allegation is untrue is clearly of significant value in setting the record straight. This publicity of the true position is a far greater motivating factor to pursue libel proceedings than a monetary outcome, although the courts can award damages and costs. Orders for removal of content may also be made, including against third parties such as social media platforms.

Practical effect

When dealing with disparaging statements made online, especially on social media, it is important for the adviser to be able to provide some objectivity. The subject will understandably be upset by what has been said about them, but it is key to evaluate the true impact of an online allegation. Does the online location have significant reach? There is little point in a complaint about a tweet with a handful of followers. Does the author have any credibility, or will they simply be regarded as partisan or unreliable? Is the statement made in an 'echo chamber' – in other words, are all the readers already likely to hold an established fixed view? Will the statement 'cut through' to the wider media? How serious is the allegation – merely rudeness or insult, or a claim that strikes at the core attributes of an individual? These are all factors to be taken into account when deciding when to act and when to leave well alone.

Where an allegation is credible, serious and has gained widespread circulation, this favours action. If the statement is preventing an individual from continuing life or business as usual, damaging friendships or leading to lost business or employment opportunities, then action may become essential.

Online harassment

Defining 'harassment'

Online harassment can manifest in a number of ways, such as:

- repeatedly sending unwanted messages, whether to an individual directly and/or to someone connected to them;
- repeatedly posting information about the target;
- cyberstalking; or
- impersonating the target online.

This may or may not be combined with analogue harassment (eg, letter writing) or in-person harassment and stalking. This can cause significant distress and may also result in risks to personal safety. There are a number of specialists who can assess and analyse a harasser's activity and advise on risks and the best course of action for containing the threat and bringing the campaign to an end. Seeking specialist psychiatric advice on the harasser's motivation and aims can assist in setting a strategy, in conjunction with the victim's lawyers and other professional advisers, to respond most effectively to the harassment.

Section 1 of the Protection from Harassment Act 1997 makes it both a criminal and a civil offence to pursue a 'course of conduct' (two or more instances) that amounts to harassment of another person, and which the harasser knows or ought to know amounts to harassment. While the term 'harassment' is not defined within the 1997 act, Nicklin J held in *Hayden v Dickenson* [2020] EWHC 3291 (QB) at para 4:

> *Harassment is an ordinary … word with a well understood meaning: it is a persistent and deliberate course of unacceptable and oppressive conduct, targeted at another person, which is calculated to and does cause that person alarm, fear or distress … The behaviour said to amount to harassment must reach a level of seriousness passing beyond irritations, annoyances, even a measure of upset … To cross the border from the regrettable to the objectionable, the gravity of the misconduct must be of an order which would sustain criminal liability …*

Defences to a claim of harassment

Defences to claims of harassment include where the conduct:

- was pursued for the purpose preventing or detecting a crime; or
- was 'reasonable' in the particular circumstances.

In assessing claims under the 1997 act, the courts will balance the rights and interests of the parties, as well as the public interest. While most instances of harassment and particularly online harassment do not involve journalists, such claims are helpful in providing insight into how the courts balance public interest in harassment claims and what is considered 'reasonable'. In *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233, the Court of Appeal held that while publications in a newspaper are capable of amounting to harassment, "In general, press criticism, even if robust, does not constitute unreasonable conduct and does not fall within the natural meaning of harassment". [2]

Available remedies

The 1997 act allows victims of harassment to seek injunctions, damages or both from their harassers in the civil courts. Where granted, injunctive relief will usually prohibit the harassers:

- from continuing or repeating the harassment; or
- from contacting or approaching the victim, whether directly or indirectly.

While damages are very rarely the motivating factor in bringing a claim in harassment, these may be awarded to compensate the victim for:

- the anxiety or distress suffered;
- loss of dignity; and
- financial loss suffered as a result of the harassment.

Criminal offences under the 1997 act for harassment or putting someone in fear of violence can result in fines, imprisonment or both.

2 The Independent Press Standards Organisation (IPSO), the independent regulator of most of the newspapers and magazines operating in the United Kingdom, recognises that there are some circumstances in which press enquiries can become oppressive and unreasonable; it operates a 24-hour emergency harassment helpline. IPSO's Editors' Code of Practice also provides that journalists must not continue to question, contact or photograph people once they have been asked to stop doing so, unless there is specific and adequate public interest to justify a decision to carry on.

Communication offences

While the rise in online and electronic communications has in many circumstances positively reshaped the way we engage with each other, it has also created new associated risks requiring parity in the way that online and offline offending are tackled by investigators and prosecuting authorities.

The need to uphold one's right to freedom of expression is fundamental.[3] However, where communications sent convey a message, threat or information which constitutes a criminal offence, investigators and prosecuting authorities will intervene when reasonable and proportionate to do so.

Potential criminal offences – online communications

Electronic communications sent via social media may result in the commission of a range of criminal offences, including:

- offences against the person and/or public justice;
- sexual or public order offences;
- harassment;
- stalking; and
- controlling and coercive behaviour.

However, a starting point for investigators will often be whether an offence has been committed under the specific communication offences – namely the Communications Act 2003 and/or the Malicious Communications Act 1988.

To establish whether a communication offence has been committed, one should consider:

- the language used;
- the period over which the communications have been sent;
- any relevant context and background between the parties; and
- whether there are other associated criminal offences.

3 Article 10 ECHR

Communications that are grossly offensive, indecent[4], obscene[5] or menacing in character[6] will often satisfy the requirements under the legislation. If a party sends a communication which they know to be false or persistently use a public electronic communications network which causes annoyance, inconvenience or anxiety, this may also constitute a criminal offence.[7] It is not necessary to show that a message was addressed to or received by another person; the offence is committed when the message is sent and also covers reposting and sharing.[8]

Cyberstalking

There is no legal definition of 'cyberstalking' or specific legislation to combat this behaviour. Where it is identified, investigators will often seek to pursue comparable offences such as stalking, harassment and/or communication offences and controlling and coercive behaviour. Examples of cyberstalking include:

- spamming, where a party sends another multiple junk emails;
- 'baiting', or humiliating a party online by them as sexually promiscuous;
- trolling;
- leaving improper messages on online forums or message boards;
- sending electronic viruses; and
- posting photoshopped images of persons on a social media platform.[9]

Cyberstalking against women and girls has been recognised by prosecuting authorities as a form

4 *Connolly v DPP* [2007] 2 ALL ER 1012 defined 'grossly offensive' and 'indecent' as taking their ordinary meaning in the English language.
5 *R v Anderson* [1972] 1 QB 304 defined 'obscene' as taking its ordinary meaning in the English language
6 *Chamber v DPP* [2012] EWHC 2157 defined 'menacing' as creating a sense of apprehension or fear.
7 Section 127(2) of the Communications Act 2003.
8 *Chamber v DPP* [2012] EWHC 2157.
9 Legal guidance on social media and other electronic communications issued by the Crown Prosecution Service, updated 2023.

of "discrimination against women and a fundamental issue of human rights arising from gender inequality".[10] Where there is evidence of cyberstalking against women or girls, prosecutors should consider the specific policy and guidance[11] issued in this area, being mindful not to make assumptions about the gender, age, race or socio-economic background of the victim when building their case.

Reporting a crime

Where a person suspects that an offence has been committed, it is beneficial to preserve the communication where possible and they should be prepared to supply this to investigators when filing a criminal complaint. It may also be useful to keep a record of the dates and times at which any messages were sent; where there is a risk of these being removed or lost, it will help to take a comprehensive note of the message itself and its contents.

Where a person is the victim of an anonymous post, it may often prove difficult for investigators to identify the culprit. The speed at which a culprit may be identified will depend on the cooperation of the social media company hosting the site on which the message has been sent.

Where the culprit is anonymous, it is worth keeping a record of the name used on the account posting and identifying any distinguishing features of it, including any contacts/friends associated with the account and those who have liked or shared any messages.

Despite a rise in complaints in relation to online offending, there are often delays between complaints being made and an outcome being determined by the prosecuting authorities. This is blamed on a lack of resourcing and investment in public services, as well as the evidential and legal complexities involved in investigating these cases. In 2021 the Law Commission published recommendations[12] to modernise this area, which have been accepted by the government and are likely to be included in new legislation[13] aimed at tackling the many pitfalls faced by investigators and prosecutors when handling these cases.

Inaccurate or out-of-date search engine results

The distinction between de-indexing and removal

Some aspects of data protection law have become surprisingly well known. One of these is the so-called 'right to be forgotten'. It is helpful to understand what this means in practice, as it is somewhat more limited in scope than the name might suggest.

'De-indexing' means the removal from a search engine list of the snippet and the link to content being hosted elsewhere. If a URL is de-indexed, the content still exists and sits at its original location and can be viewed; but it cannot be navigated to by using a search engine. This can be practically valuable because of the immense influence of Google in finding content online.

This is to be contrasted with removal of content at source, which means that the party with control of the URL deletes the page or content, so it can no longer be viewed at all. It will drop out of search engine results, although this can take a short while to take effect; but in the meantime, any result will direct only to a broken link.

Legal basis

The right to be forgotten now has its legal basis in Article 17 of the EU General Data Protection Regulation (2016/679) (GDPR), which is directly applicable within the European Union and continues in the United Kingdom by virtue of the European Union (Withdrawal) Act 2018. An individual may seek the erasure of personal data by the data controller on a number of grounds, but those of most relevance to online content are that:

10 Violence against women and girls guidance published by the Crown Prosecution Service updated 2019.
11 Violence against women and girls guidance published by the Crown Prosecution Service update 2019.
12 Reform of the Communications Offences published by the Law Commission dated 2021.
13 The Online Safety Bill and the Online Safety Act 2023.

- the personal data has been unlawfully processed; or
- the data subject objects and there are no overriding legitimate grounds for the personal data to continue being processed.

It is far from an entitlement to removal of content that is merely objectionable or offends; and there is an express exemption for freedom of expression.

The factors that Google lists as relevant to its decision on whether to de-index content are:

- a person's role in public life;
- the source and the age of the content;
- whether it is true or false;
- whether the information is highly sensitive; and
- whether there is a public interest reason for making the content available.

Value

Careful consideration should be given to any removal request before it is made, as it can have unintended consequences and, when ill used, can make a reputational situation worse. The removal of inaccurate or out-of-date personal data should not end up giving the appearance of 'airbrushing' a reputation or covertly altering history. If facts are wrong, it may be better to address a complaint to the original source of the claim rather than trying to de-index content from search engines. Sometimes this is not possible because of the nature or location of the source, which may be a reason to de-index. Always consider that removal of content may in itself attract attention and could cause critics or opponents to create new content or repeat the same claims.

The right of erasure is only given effect on Google to search results within the European Union, so for global individuals its value may also be limited for this reason.

Misuse of private information online

What amounts to a misuse of private information?

The tort of misuse of private information is a relatively recent development in English law, arising from the incorporation of the European Convention on Human Rights (ECHR) into domestic law by the Human Rights Act 1998. The tort protects the right to respect for private life and family, home and correspondence under Article 8 of the ECHR.

To bring a claim for misuse of private information, a claimant must establish that:

- they have a reasonable expectation of privacy in relation to the information in question; and
- the disclosure or publication of the information was not justified by a countervailing public interest or right to freedom of expression under Article 10 of the ECHR.

When does an individual have a reasonable expectation of privacy?

The following are categories of information in respect of which a person may have a reasonable expectation of privacy:

- financial affairs;
- health records;
- personal relationships, including romantic and sexual relationships;
- family matters;
- security arrangements; and
- personal correspondence.

The Supreme Court has also recently affirmed that where an individual is under investigation by the police, the general rule is that they will have

a reasonable expectation of privacy in respect of information relating to that investigation up until the point of charge.[14] Whether an individual enjoys a reasonable expectation of privacy will always require a detailed and fact-specific assessment of the particular circumstances. If a claimant has consented to disclosure of the information in question, or if the information is or was already in the public domain at the time of the (intended) publication, the claimant's expectation of privacy will be reduced.

When can interference with an individual's privacy be justified?

Online interference with a claimant's reasonable expectation of privacy through disclosure or publication of the private information may be justified in the following non-exhaustive circumstances:

- The disclosure or publication of the information contributes to a debate of general interest and/or exposes wrongdoing or hypocrisy;
- The disclosure is made in the course of legal, parliamentary or judicial proceedings and has been reported fairly and accurately online; or
- The discloser has a legal, moral or social duty or interest to communicate the information to a specific recipient or a limited audience, which has a corresponding duty or interest in receiving that information, provided that the discloser is not acting maliciously and with an improper motive or in the knowledge that the information is false.

In conducting a balancing act between Article 8 and Article 10, the courts will have regard to:

- the proportionality and necessity of the interference with the claimant's privacy; and
- the nature and extent of the disclosure or publication.

In doing so, the courts will take into account factors such as:

- the nature and source of the information;
- the purpose and manner of the disclosure or publication;
- the impact on the claimant's dignity, autonomy and reputation; and
- the contribution of the information to a matter of public debate.

The courts place particular import on the Article 8 rights of children; in the case of the offspring of a famous parent, the courts have accepted that interference with a child's right to privacy might give rise to greater safety and security concerns, and that considerable weight should be given to a child's best interests in conducting the balancing exercise between Article 8 and Article 10. [15]

PJS v News Group Newspapers Ltd [2016] UKSC 26 is an example of where Article 8 was held to outweigh Article 10. In this case, the Supreme Court granted an injunction to prevent the publication of details of a celebrity's extramarital sexual encounters, finding that there was no public interest in exposing his private life, and that the injunction was effective despite the information being available (including online) in other jurisdictions. While PJS obtained injunctive relief in England and Wales, the remedy was only effective in this jurisdiction and not globally; by the time the injunction was obtained, the unjustified disclosure of his private information had spread in other countries.

What remedies are available?

The main remedies available under the tort of misuse of private information are injunctions, damages and delivery up or destruction of the information. Injunctions can be sought to prevent or restrain the disclosure or publication of information, or to require the removal or deletion of information from online platforms. Damages can be awarded:

- to compensate the claimant for:
  - distress, loss of dignity and autonomy over the use of their private information; and

14 *ZXC v Bloomberg LP* [2022] UKSC 5.

15 *Weller v Associated Newspapers Ltd* [2015] EWCA Civ 1176.

- financial harm caused by the misuse of private information; and
- to vindicate their rights.

Delivery up or destruction may be ordered to prevent further misuse or dissemination of the information which is the subject matter of the claim.

Impersonation online

How can impersonation manifest online?

Impersonation online can cause significant reputational damage. Those in the public eye and HNWs are more likely to be targeted in this way, due to both their higher public profile and the potential for more lucrative blackmail/extortion demands in exchange for release of profiles or desisting from further unauthorised use of the victim's details. Similarly, there is a significant reputational risk for corporate entities, and those with which they are associated, if the company's details are misappropriated and used without authority to perpetuate a fraud or otherwise engage in wrongdoing.

What causes of action may be relevant?

In England and Wales, there is no specific statutory offence of identity theft or impersonation, except where someone is impersonating a police officer with intent to deceive.[16] However, there are various legal causes of action that may be relevant, depending on the nature and consequences of the online impersonation. These include the following causes of action discussed above:

- the tort of misuse of private information;
- defamation;
- harassment; and
- blackmail/extortion.

In addition, under the Data Protection Act 2018 and the GDPR, individuals have rights and remedies in relation to the processing of their personal data, such as:

- the right to access, rectify, erase, restrict or object to the processing; and
- the right to compensation for any damage or distress caused by a breach of the data protection principles or rights.

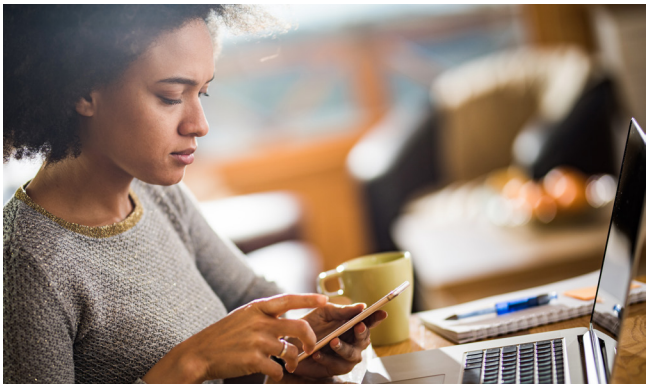
Most websites, including major social media sites, prohibit impersonation under their user terms and this can offer a legal basis for removal of such content. Where the victim is a corporate, rather than an individual, there may also be causes of action relating to unauthorised use of the victim's IP rights.

Combating misinformation and impersonation

In addition to any legal steps which it may be appropriate to take, it is also important to consider whether to seek to publicise and counter online impersonation in order to combat any reputational damage. This is particularly important where an impersonator is seeking to deceive third parties; lack of action in alerting others to the false impersonation once on notice of the impersonator could expose the victim to significant criticism.

Privacy planning

If you accept the general proposition that reputation is a valuable asset in society, it follows that it deserves active management and protection like other asset classes. Again, as with other assets, its value may increase or decrease over time, and sometimes as a result of circumstances beyond the subject's own



16 Section 90(1) of the Police Act 1996.

control. However, that doesn't mean that there is no point in thinking about how personal information is presented to the world at large. If a person is at least aware of what makes up their digital footprint, there is scope to make sure that it is accurate and in line with the subject's own desire for privacy or openness.

Charlie Bain, managing partner of digital risk and online reputation consultancy Digitalis, explains:

> *For high-profile businesspeople, knowing what's out there online about you in granular detail is essential. Most of our clients know about 60% of what is online about them but are staggered when we show them the remain 40% and how it can be used against them.*
>
> *The culture of creating and sharing content over the last 15 years or so now means almost everyone has an extensive digital footprint. This 'digital library' of our lives is gold dust to someone with malintent.*
>
> *Now that could be a hostile journalist but more often than not these days it's a disgruntled former employee, hostile political activist, angry shareholder, or member of the public with a grudge – anybody who wants to cause harm can find a way to get hold of that content and highlight it in a derogatory way.*
>
> *One of the critical areas of digital privacy invasion which most people forget is that it's often not the platform you post on which causes the issue, it's the publication, outlet or individual that spots it, finds the angle and uses the content to repurpose it into a damaging story or posting.*

While a periodic review may be advisable, there are likely to be specific points at which assessing an online footprint is critical – for example, prior to major life events or professional developments, such as:

- appointments to public office;
- donations to political parties or charities; or
- business acquisitions.

One area that frequently arises is public domain information concerning a private home including interior photographs, floorplans and full address. While this content is inoffensive, it may be entirely inappropriate in the case of the home of a high-profile individual and could compromise their physical safety. This is precisely the type of information that could justify action to obtain removal.

The extent to which otherwise private information is put into the public domain may depend heavily on those around the individual, such as family members and employees. Disclosures may be capable of control by means of appropriate contracts being put in place (although these should always permit proper public interest disclosures of a whistleblowing nature). Among high-profile families, an inter-generational discussion is highly recommended with a view to finding a suitable balance that might accommodate both a senior statesman and a social media influencer within the same family.

Conclusion

The Internet and technological advances present new challenges for those seeking to protect their reputation and privacy. However, the Internet also provides new opportunities for individuals and companies to communicate more effectively, shape perception and define their own reputations.

There is a common misconception that the Internet is a Wild West beyond the reach of the civil courts and law enforcement agencies. However, this is not the case and governments across the globe are legislating to ensure that rights are protected and remedies available where unlawful conduct occurs online.

Active steps can be taken to reduce reputational risks through proactive planning and by ensuring that risks are identified and addressed when they arise.