Remote working in a time of crisis

By Allan Carton

Advice from the MD of Inpractice UK on coping with the current crisis, with insights from several other PMS suppliers.

The impact of Covid-19 is being felt by all of us to varying degrees. People should work from home if they can but that may not be possible yet for everyone in your practice. As many of you will be doing this already, there is advice here to help refine that experience. Also, on the different set of challenges that everyone will face now to maintain a healthy working environment for people not used to working from home in relative isolation.

Seek advice

Firstly, make sure you have someone to talk to and work with. This situation is new for most firms, so the leaders in your practice need to be talking to someone to help – both in relation to the tech you use and mindsets.

To keep in tune with the thinking of your peers in other professional practices, you can sign up for a series of webinars on Inpractice being chaired by Richard Chaplin, CEO of the Managing Partners’ Forum, where leaders in legal, accountancy and similar practices candidly share their experience of coping with the impact of Covid-19 (www.inpractice.co.uk/events).

The two applications that virtually every firm in the country works with are: some version of the Microsoft Office suite of products – Word, Excel etc; and some practice management system (PMS). Of course, there are many other legal applications and tools, but these are the core. The PMS providers are keen to help, so talk to them in addition to any business that manages your IT systems for you or hosts them. They all recognise that we are in this together.

If you are hosted, rather than using servers located on your own premises, you are likely to be in a better position right now to provide access to your people to work from home as that facility is an integral part of your solution – but that doesn’t deal entirely with challenges on the softer side of moving all your people to work from home permanently for the length of time likely to be needed now.

Shared insights

To add to our own advice we gathered recommendations from a selection of legal practice management system (PMS) suppliers (Insight Legal, DPS, Advanced Legal and Tikit for starters, so thank you to them), incorporated in the summary below.

We all have some transition to make to full home working, even here at Inpractice where we have used hosted service and home offices across the country for more than 10 years. How even we work has changed dramatically in just the last week because many of our clients are doing it too for the first time – as are your clients.

Hopefully these prompts and reminders are helpful.

Don’t panic. Transitioning to cloud based or getting a new system up and running can be done relatively quickly. If you need to change provider or get a system in place, speak to someone now. Adapting quickly doesn’t mean you have to be tied in for years
with a provider. However, you still want to do this properly so try to ensure that what you choose now is workable and fits with how you will work in the future. This experience has the potential to be the catalyst that will result in more effective home working and online collaboration for many in the future.

Post a succinct and clear message on the home page of your website to inform clients what your firm is doing to maintain business as usual during this time. Be prepared to change it regularly to keep it up to date.

Find a quiet place in your house to work and make it your office. Be prepared to buy or tell people to take home an ergonomic chair so that you can all work comfortably. You need to be able to work there in comfort for probably the next 3 months. When using your laptop for video conferencing, raise it up to your eye line so you look straight at people – and be aware of what is behind you.

Get some workable video conferencing up and running as soon as you possibly can so people get comfortable with it. Focus more on this as a critical first step to get up and running. This will make everything else much easier to implement.

The simplest options are probably Zoom and Skype, but there are others too of course – even Facetime, where it is possible to hold group meetings with others using iPhones, iPads etc. Zoom and Skype are easy and free to run most of the meetings you will need with anyone inside or outside your organisation “at the drop of a hat”.

Zoom is free for all one-to-one meetings and for group meetings up to 40 minutes long. Your clients are likely to be using either of these too and they are very user friendly. Don’t hesitate to try them and be willing to use them with clients too, who will appreciate your efforts. We are all in the same boat.

This does mean that you want your people to have fast broadband access at home to get the best quality reception and a decent laptop with a camera, microphone and speakers that work.

Wireless headsets with noise cancelling can connect by Bluetooth to both your mobile (which you can use for any of the video conference apps mentioned above) and your PC or laptop – and you can listen to music too while you work or wait for calls to come in. That helps to reduce the distractions created by others around you at home. It might be a boost for some to provide these and they will likely come in useful in the future for many at home anyway. I use (high end) Bose headphones, but there are less expensive and less obtrusive options that many may prefer.

Get a sound remote working policy in place. Make sure you know who is supplying the equipment for home use, whether it is included in your insurance, where any liabilities lie for health and safety. Your remote working policies should refer to your suite of general IT security and GDPR / privacy policies. Continuing the discussions with your team will help to refine your approach to how people can work best over time, so keep this on your agenda and work continuously on a list of improvements.

Plan your day to do what you do at work. Walk around, talk to people, make a drink, have a lunch time. It’s very easy to really go over the top and check emails and work on documents for 14 hours a day simply because it’s at hand and you can. Plan not to.

Increase the use of voice and video contact during a time when we will all be feeling increasingly isolated. We all need to adopt a more human type of contact during this crisis to keep spirits up. It helps to do this through regular scheduled one-to-one and group meetings.

Actively schedule “down time” group meetings online to help people relax and share each other’s company and news. This is critical and can be readily bypassed. Don’t let that happen.

Make sure laptops, PC’s and broadband accessed through home routers are secure. It would be useful to provide a good password manager like Dashlane (which we use) or LastPass as people will otherwise be tempted – when in a hurry – to re-use passwords for ancillary apps and online services that can put them at risk. Implement two-factor authentication also wherever you can.

There is of course much more to be said about protection against cyber threats but these are at least a good starting point. For more depth, implement Cyber Essentials at home (www.cyberessentials.ncsc.gov.uk).

Start using more of the right software to help you work online. Not all employees are going to be tech savvy, so you want to make it as easy as possible for them to connect, so that employees don’t need to download or install anything. They want to just open their browser and log in. See the discussion of Microsoft tools below.

Plan and talk about workloads. Ensure that staff have enough work to be getting on with at home, ensure that they are capable and have the right support available. Using tools such as Microsoft Teams can be invaluable in enabling them to collaborate with colleagues on their work.

It helps to know what work your people are handling so you can help them. Use the tools available

Internet Newsletter for Lawyers is edited by Nick Holmes and published by infolaw Limited
ISSN 2046-9284. Personal Print+PDF subscription (6 issues) £50. Multi-use £80+VAT
Subscription information and online access are at www.infolaw.co.uk/newsletter
Subscription enquiries to infolaw subscribe@infolaw.co.uk 5 Coval Passage, London SW14 7RE Tel 020 8878 3033
For all editorial, advertising and publishing enquiries, contact Nick Holmes nickholmes@infolaw.co.uk

Thanks to our online sponsors
Eclipse (www.eclipselegal.co.uk) – The only PMS solution endorsed by the Law Society
Bloomsbury Law Online (www.bloomsburylawonline.com) – Fully searchable, instant access to expert content
in your practice and case management system to set the agenda for regularly scheduled work-based discussions.

**Communicate online now with clients – don’t wait.** They are in the same boat and as unsure about the next steps as you are. Share your feelings, concerns and plans. Ensure that all clients are aware of the changes being made in your firm and that there will be changes in the way you communicate as a result. Ensure all communications are through a secure channel as now is a great time for a cyber-criminal to call a client pretending to be from your firm with a change in bank details.

**Tools to bundle documents can play a significant part** in making it easier to share documents online with clients, counsel and colleagues. It is worth checking out what is already available from your PMS provider to do this as we tend to find that many firms are just not aware of what is possible.

**Keep your thinking on business development going.** Working this way will open your eyes to new opportunities to do things differently for the better in the future. At some stage – if not immediately – this will give you an opportunity to plan and begin to implement some initiatives that you have put on the back burner in the past. Steps that will now help you to bounce back when the time comes … as it will.

**Introduce ways to securely share documents online** for your clients to check, complete and sign electronically and they can do likewise – either through your PMS or third-party applications.

It is also time to **set up fall-back arrangements** with tried and tested suppliers with reliable services that give you options to outsource book-keeping, call handling and dictation.

Also, **make more and better use of online applications** for ID verification, AML compliance, client onboarding, conveyancing quote conversion.

**Microsoft tools**

If you have been following Inpractice advice over the last 18 months or so, you will be using some variation of Microsoft **Office 365**, with the various options outlined here. Some of these include Microsoft **Teams** which gives you all the video conferencing service you need (and much more).

In response to the Covid-19 outbreak, Microsoft currently offer a free 6-month trial of the full paid version of Office 365 E1, which includes Teams. If you don’t have Office 365 yet or Teams, please check this out first.

However, many firms already using Office 365 use it just for Word and Excel but have not yet managed to configure, train or use much of the video conferencing and other collaboration features included in the subscription.

Now you are probably going to have to dive in quickly to get that working – not just within your practice, but also to make use of all these invaluable features to communicate and collaborate with clients.

Perhaps some time out now will be the catalyst and incentive to get this working for you in the short term, but with longer term benefits for your practice too?

Office 365 includes **SharePoint** too, which can readily be configured to share any type of document. You can use it to share policies, procedures and other important documents if you currently can’t do this through your PMS. There would be some cost to set it up but no ongoing licencing costs and universal access for everyone.

With these Microsoft tools available there is much more you can do, such as setting up a “crisis communication platform”, but that’s probably for another day when your people have more time to think through how best to make it work for you.

Allan Carton is Managing Director at **Inpractice UK**, helping legal practices tap into new business opportunities and develop new propositions, better CRM, client management and improved processes; all making better use of technology.

Email acarton@inpractice.co.uk, Twitter @AllanCarton.

Image cc by jofalltrades.com on Flickr.

**Free initial advice from Inpractice UK**

For free initial advice from Inpractice UK you can book a time for a 30 minute call or video conference with us [online](#) or call us on 0161 929 8355.
Electronic witnessing of documents

By Chris Bryden

On 3 March 2020 the Lord Chancellor, Robert Buckland QC, made a written ministerial statement welcoming the report of the Law Commission on Electronic Execution of Documents (Law Com No 386). That report concludes that there is no need for formal primary legislation to reinforce the legal validity of electronic signatures on documents, and that the existing framework makes clear that businesses and individuals can feel confident in using e-signatures in commercial transactions. This is consistent with guidance given by the Law Society on 21 July 2016 and established practice, and supported by case law.

Automatic signatures

In the recent case of Neocleous v Rees [2019] EWHC 2462 (Ch) the High Court considered whether an automatic signature on an email was sufficient to render a document signed within the meaning of section 2(3) of the Law of Property (Miscellaneous Provisions) Act 1989 (“the 1989 Act”). The 1989 Act provides that a contract for the sale or disposition of an interest in land must be in writing and the documents incorporating the terms must be signed by or on behalf of each party to the contract. The Claimant sought specific performance, contending that a series of emails amounted to contractual terms and that the electronic signature automatically added to the emails complied with the requirements of the 1989 Act. The court agreed. Reference was made to relevant case law in this regard as well as to the Law Commission Consultation Paper which preceded its Report, and which found that the weight of the case law supported the view that an electronic signature satisfied a requirement for a signature where there was evidence of an intention to authenticate the document.

Witnessing of electronic signatures

The ministerial statement went on to reference a more equivocal matter contained in the Law Commission Report, being the question of video witnessing of electronic signatures. The statement went only so far as to ask that the Industry Working Group to be established in accordance with the Report’s recommendations, to consider this question. The issue arises in particular where the relevant signatures are made by execution of a deed, such as, by virtue of section 52 of the Law of Property Act 1925, where a transfer of land takes place. In respect of deeds, section 1(3) of the 1989 Act provides that an instrument is validly executed as a deed if, and only if, it is signed by an individual in the presence of a witness who attests the signature; or at his direction and in his presence and the presence of two witnesses who each attest the signature, and it is delivered as a deed. The particular difficulty is what is meant by “in the presence of a witness”; can this presence be virtual, or must the witness be physically present? If the latter, electronic execution of a deed would require the presence of an attesting witness alongside the electronic signor.

This issue arose in Man Ching Yuen v Landy Chet Kin Wong [2019] UKFTT 2016/1089 (Tribunal Judge Gatty), in which the writer appeared for the Respondent. The matter concerned a residential property which was registered in the sole name of the Respondent by virtue of a Form TR1 dated 30 September 2010. The Applicant, who had previously been registered as a co-owner, lodged a unilateral notice against the title. The Respondent applied to cancel the notice, to which the Applicant objected, leading to the referral of the matter by the Land Registry to the First Tier Tribunal.

There was a significant factual dispute in respect of the Form TR1. It was not in dispute that such a form existed. It purported to be signed by both Applicant and Respondent, and to have been witnessed by a solicitor. However, the Applicant denied that he has signed the document at all, contending that it was a forgery. The Respondent’s case was that the parties had met in her office in Hong Kong, and had both signed the Form TR1. The attesting solicitor had been virtually present via Skype, had witnessed the signatures of both parties, and, when the Form TR1 was later received by her in the post, she added her attesting signature to the document.

The factual dispute was disposed of in favour of the Respondent, primarily on the basis of the evidence of the attesting solicitor. At paragraph 20 of the judgment the Tribunal Judge recorded that she had asked to see proof of identity and was shown a Hong Kong identity card with a photograph on it, but was concerned that this had no expiry date and thus asked to see a bank card, which she was shown, with a matching signature to that placed on the Form TR1. The Tribunal dismissed the prospect of the Respondent having found a look-a-like for the Applicant and forged both an identity card and, in anticipation of the request, a bank card, as this “would have required a level of cunning and criminal organisation that would be beyond most people.”

The resolution of the factual dispute was not, however, the end of the matter, as the Applicant argued that even if (which he denied) it was his signature on the transfer, the Form TR1 was not a valid deed as the attesting solicitor was not present as she was not physically there. Although the Tribunal Judge ultimately determined that he did not need to decide this question, significant analysis of the issue is contained within the judgment, as well as consideration of the findings of the Law Commission Report. As far as is known, this judgment therefore contains the most comprehensive modern analysis of the requirements of section 1(3) of the 1989 Act, viz the requirement of physical presence by the attesting witness.

Physical presence

The Tribunal Judge began by noting that the Law Commission had expressed a provisional view in its consultation paper that actual physical presence was probably required. However, he accepted the submission made on behalf of the Respondent that the final Report was more equivocal. At paragraph 5.30 of the final Report the conclusion is that “it is not clear that the requirement may be satisfied by remote forms of witnessing”; and that there is a presumption that
Parliament intends courts to interpret legislation allowing for changes including technological developments. The judgment goes on to cite paragraph 5.35 of the Report. This provides:

"Some consultees argued that it would be open for a court to decide that remote or virtual witnessing would satisfy the statutory requirements. Although we agree that may be the case, we are not persuaded that parties can be confident that the current law would allow for a witness viewing the signing on a screen or through an electronic signature platform, without being physically present. This conclusion is based on the combination of the restrictive wording of the statutory provisions and the serious policy questions underlying any extension to accommodate technological developments."

The Tribunal Judge noted that one of the factors relied upon in the Report in favour of the need for physical presence was a requirement for the signature of the witness to be affixed at the same time as execution of the deed. However, he noted that in *Wood v Commercial First Business Ltd (In Liquidation)* [2019] EWHC 2205 (Ch) the High Court had held that whilst it was a requirement that the person executing the deed sign in the presence of a witness, it is not a requirement for the witness to sign in the presence of the person executing. Having gone on to consider *Wright v Wakeford* (1812) 4 Taunton 213 and *Netglory Pty Ltd v Caratti* [2013] WASC 364 (a case in the Supreme Court of Western Australia) the Tribunal Judge held that it is not a requirement of section 1(3) that the witness' attesting signature must be made on the same occasion as the maker of the deed's signature, within a reasonable period of time, such as a few days as in the instant case. This undermined one, but only one, of the Law Commission's justifications in support of physical presence.

The Tribunal Judge did not consider on the question before him that the nineteenth century authorities were of any use as to whether "presence" could include "virtual presence" but rather framed the question as one of policy – a balancing of risk and convenience. As both the Law Commission and the Tribunal Judge recognised, the present law permits of more than one conceivable answer, and, therefore in the context of the application before him, given the uncertain state of the law, the Applicant had a realistic prospect of persuading a court or Tribunal hearing a rectification application that the TR1 was not validly executed as a deed due to the lack of physical presence. However, the Respondent succeeded overall, the Tribunal finding that, were rectification to take place, a constructive trust would arise due to the signature on the TR1, allowing the Respondent to require the re-conveyance of the Property. He therefore dismissed the application and directed that the unilateral notice be cancelled.

**Room for argument**

There have been a number of erroneous reports suggesting that this case is authority for the proposition that virtual presence is not sufficient for the requirements of section 1(3) of the 1989 Act. That is not the case. It is likewise not the case that the Law Commission Report is supportive of such proposition. Rather, what is clear both from the Report and the decision is that there is scope for argument either way and at present no authoritative determination in the case law. This is perhaps surprising given the growth of electronic signatures and virtual working. It appears conceptually surprising that contemporaneous virtual witnessing by video-link should not be thought to be as secure as the physical presence of a witness, as a matter of policy, given the purpose of a witness is to prevent against fraud, and unsatisfactory that equity may need to intervene in such circumstances where bar actual physicality the formality and policy requirements have been met. *Yuen v Wong* makes clear that there is room for argument, and that the position is not cut-cut. The finding that an argument that there be physical presence has a realistic prospect of success is a far cry from a determination that this must be the case, and the point remains open to determination. It is hoped that the Industry Working Group takes note of the considerations given by Tribunal Judge Gatty to this difficult area in a case which, though a first instance tribunal decision, deserves much wider recognition.

Chris Bryden is a barrister at 4 Kings Bench Walk, specialising in Chancery, civil and family law.

Email cxb@4kbw.co.uk. Twitter @BrydenLaw.
How healthy is your data?
By Alex Heshmaty

Can technology improve our health and transform healthcare? A whole panoply of tech companies are working on a range of products and services which aim to answer these questions in the affirmative. The burgeoning industry which has been dubbed “medtech” has already led to some fascinating (and controversial) partnerships, perhaps most notably involving Google Deepmind being granted access to NHS patient data. It has been estimated that the medical device and technology sector could be worth around $500 billion to the global economy by 2021. But despite the potential for healthy growth, there are also many concerns associated with medtech, not least in terms of data protection. These are discussed below, including a section on how health data is being used in the fight against coronavirus.

What is medtech?

Health technology is defined by the World Health Organization (WHO) as “the application of organized knowledge and skills in the form of devices, medicines, vaccines, procedures and systems developed to solve a health problem and improve quality of lives.” Medtech can encompass this very broad definition but it normally refers to the more cutting edge end of the spectrum, specifically medical devices, the application of AI to large sets of health data, online health resources and DIY biohacking. We explore some of these below.

Medical devices

Medical devices range from the widely used fitness and sleep trackers, which often just rely on accelerometers to calculate movement, all the way through to important medical gadgets such as continuous glucose monitors (CGM) used to measure the blood sugar level of diabetics (usually linked to a smartphone app which displays readings in real time) and even complex life-saving implants such as the subcutaneous implantable cardioverter defibrillators (S-ICD) which continuously monitor the heart rate of people who are susceptible to dangerous heart arrhythmia and deliver an electric shock if required. Medical devices are often internet-connected and therefore fall under the umbrella of Internet of Things (IoT).

AI analytics

The ability of analytics software to quickly process large amounts of health data and spot patterns or trends (often using an element of artificial intelligence) can help doctors diagnose patients early, often resulting in more successful treatment. Back in 2016 Google’s Deepmind teamed up with the Royal Free NHS Foundation Trust to analyse the data of 1.6 million patients. Deepmind developed an alert app to enhance the efficiency of diagnosing and detecting patients who were at risk of developing acute kidney injury (AKI).

The ability to analyse vast amounts of health data has also been touted as a boon to personalised medicine, which promises to move away from a blanket method of health provision to more effective tailored treatments. Furthermore, it can help in the fight against pandemics.

Online health

Although the proverbial “Doctor Google” is often blamed for hypochondria, the fact is that the first port of call for most people seeking health information is the internet. Google is fully aware of the scale of the health market and, not only does it make a pretty penny from advertising health products, its parent company Alphabet has its own dedicated healthcare projects such as Verily and Calico.

Babylon Health has been lauded as one of the world’s first regulated virtual health primary care providers, with its GP at Hand service serving over 75,000 patients. It heavily relies on chatbots and AI to diagnose medical conditions, although it also employs doctors who can talk to patients via the app or even make face to face appointments. It is regulated by the Care Quality Commission (CQC).

Biohacking

The move towards technological methods of healthcare and the availability of technical information online has led some individuals to attempt to hack their own health, eg by customising their own medical devices. This is often a reaction to the slow-moving healthcare regulatory system, but some individuals (known as grinders or transhumanists) go further in an effort to extend their lives.

Legal concerns

The two primary regulatory issues surrounding medtech are patient safety and data protection.

Patient safety

Snake oil salesmen gained prominence in the American frontier, and there are fears that quackery is now promoting technology as a cure-all in the new Wild West of the internet. Even if we set aside the plague of online adverts and spam emails which promise a whole array of health miracles with sometimes deadly side effects from dubious sources, the regulated medtech sector is also constantly facing allegations that technological products and services are putting the health of patients at risk.

BBC’s Newsnight of 25 Feb 2020 interviewed Dr David Watkins, a consultant oncologist at The Royal
Marsden Hospital, who expressed concerns over the effectiveness of Babylon Health's AI-based triage chatbot. Although their chatbot services are registered with the Medicines and Healthcare products Regulatory Agency (MHRA) and CE marked as Class I medical devices, Dr Watkins has described this as “meaningless” in terms of providing any reassurance for patients.

Data protection

Under both the GDPR and DPA 2018, health data is categorised as "special data" which essentially means that it is subject to tighter protections as opposed to more general forms of personal data. In theory, this makes it more difficult for medtech companies to justify getting access to patient data, although the previously-mentioned deal between Deepmind and the NHS initially went under the radar without public consultation. (The hospital trust involved was later censured by the ICO for not doing enough to protect patient privacy.) In practice, many health tracking apps are gaining vast troves of personal data and potentially monetising much of this highly sensitive information by sharing it with third parties such as Facebook.

But the dilemma with data protection in the realm of healthcare is that the effectiveness of analysing health data is generally enhanced by bringing other forms of personal data into the mix. For example, having access to an individual's food shopping habits, their visits to the gym and expenditure in pubs will be able to provide a better narrative and put their overall health into context. However, merging consumer data with more sensitive data is exactly what regulators worry about in terms of protecting the public. Finding the right balance may be one of the big challenges for Silicon Valley if it intends to successfully move into the realm of health.

Coronavirus

The Coronavirus (or Covid-19) has created one of the biggest international healthcare challenges in over a century. Effective data gathering and analysis is one of the most important tools which can be used to tackle the spread of the virus, and also to understand how it works. The WHO has repeatedly emphasised the significance of mass testing of the global population to try and stymie the pandemic, and the UK government has recently announced the purchase of millions of home testing kits which can detect if someone has Covid-19 antibodies and is therefore at less risk of catching it again or spreading the virus to others.

Many countries are making available data to the public which shows the Coronavirus hotspots, where clusters of cases have been detected. South Korea, hailed as one of the countries which has been most effective in slowing the spread of the virus, has even disseminated information about the movements of individuals who have been tested positive for Covid-19. In normal times, this type of intrusive surveillance, let alone making such personal data publically available, would be seen as a huge overreach of the state and a blatant data protection breach. But desperate times call for desperate measures, and it seems that more authoritarian regimes where citizens are generally more compliant with government decrees are faring better in dealing with the pandemic. If tracking the movement of the general population via their mobile phones is effective in stopping the spread, then concerns about data protection may have to take a temporary back seat.

Tracking of citizens aside, there are many other ways in which data can be used to better deal with the situation. The Oxford Covid-19 Government Response Tracker counts data from countries around the world, in an effort to "systematically record government responses worldwide and aggregate the scores into a common 'Stringency Index'" which is designed to "help researchers, policymakers and citizens understand whether increasingly strict measures affect the rate of infection, and identify what causes governments to implement stricter or less strict measures." Meanwhile, epidemiologists and data scientists are using machine learning to analyse big data sets, in order to predict the spread of the virus and inform public health policy decision making. Google, which previously ran a Google Flu Trends prediction service, has now teamed up with Carnegie Mellon University researchers who are aiming to forecast the spread of coronavirus infections.

The coronavirus crisis is demonstrating the true value of personal health data in terms of public health. It is also raising some very interesting questions around the limits of data protection and achieving the correct balance between the right to privacy and public safety.

Further reading

FT: Can we ever trust Google with our health data? [https://on.ft.com/2y7YvdP](https://on.ft.com/2y7YvdP) (paywalled)

Alex Heshmaty is a legal copywriter and journalist with a particular interest in legal technology. He runs Legal Words, a copywriting agency in Bristol [www.legalwords.co.uk](http://www.legalwords.co.uk).

Email alex@legalwords.co.uk. LinkedIn [alexheshmaty](https://www.linkedin.com/in/alexheshmaty/).
Image: public domain from [Pikrepo](https://www.pikrepo.com).

Books


As the coronavirus pandemic spreads and courts around the world are closing, Remote Courts Worldwide was launched 30 March. It has been designed to help the global community of justice workers – judges, lawyers, court officials, litigants, court technologists – to share their experiences of remote alternatives to traditional court hearings. See [https://remotecourts.org](https://remotecourts.org).

On Prof Roger Smith's Law, Technology and Access to Justice blog, an article by Dr Simon Davey for the legal advice sector on Getting through this and moving forward – learning and sharing in a time of coronavirus. [https://law-tech-a2j.org](https://law-tech-a2j.org).

Also published, fully linked, at [www.infolaw.co.uk/newsletter](http://www.infolaw.co.uk/newsletter)
Digital marketing during a downturn

By Susan Hallam MBE

The dreaded Covid-19 is causing panic, and as digital marketers, we may be facing leaner times as our businesses are putting a laser focus on profitability, and ensuring every cost gives the great return on investment.

Businesses are looking more carefully at budgets, making sure we can squeeze every penny of profit out of our investments, and looking for the most cost-effective ways of delivering our products and services. Marketing budgets may appear to be a soft target for businesses looking to make budget cuts. But a cut in marketing activity is a short term fix that is sure to have long term consequences. Maintaining visibility in your market is essential for long term profitability and continued investment.

And our customers are also watching the pennies, but they are still spending money. They may be spending less, but we need to figure out what they're spending their money on. And they don't want to risk wasting a penny. They want to buy the right products, from companies they can trust.

Here are our five top digital marketing techniques to power your way through the crisis.

1. Work smart to retain your existing customer base

Out of sight means out of mind. You need to keep in touch with your customers or you risk losing them. And it is always cheaper to retain an existing customer than acquire a new one.

**Marketing automation** is the lowest cost, easiest, and most effective way of keeping in touch with your customers. I'm not talking sending automated email marketing spam, nor am I talking about broadcasting cold calling messages to get new customers. You need to be sending out personalised, contextualised, targeted messages to existing customers who want to hear your news. You need to be keeping in touch with your customers at every touchpoint in their digital journey through social channels, through exploring the web. And doing this systematically and automatically will ensure the job gets done, and will free up your more expensive human talents to deliver creative campaigns that will add even more ROI.

**Content production** is an essential ingredient for your tactical marketing campaigns for keeping in touch with your existing customers. Share the innovations that you are currently making that differentiates your offering from your competitors, and promote your good news stories in terms of awards and client wins. For inspiration for a B2B content marketing campaign, take a look at our article at [http://bit.ly/hallamB2B](http://bit.ly/hallamB2B).

**Getting more social** means engaging in conversations with your existing customers. LinkedIn, Twitter, Facebook: these are places where you customers are reviewing your products, discussing their purchasing decisions, exchanging views on your business. Create a low-cost plan for reaching customers at every point in the social media funnel. Use these tools to listen to your customers, hear what they’re talking about, learn more about your market. And remember it isn’t about advertising – your contributions to the conversation need to be valuable and appropriate.

2. Get even more visible in front of your potential clients

You have to build your brand awareness and get more visibility, which means driving visitors to your website to make the sales. And one of the best times to get found by potential clients is when they’re searching for what you’re selling. You need to get found at every stage of the purchasing lifecycle, from exploring new suppliers to evaluating specific offerings.

**The Mere Exposure Effect** is the marketing phenomenon by which consumers develop a preference for your products or services merely because they are familiar with them. Now is the time to explore low-cost techniques that will keep your brand visible in front of potential clients on a steady basis. It may feel counter-intuitive, but setting aside an advertising budget for keeping your brand visible will deliver long term benefits. Focus on creating high-quality content that is going to get shared, and reduce your budget for generating low value, low impact content.

**Update your evergreen content.** Your business has an archive of perennially relevant, interesting content that does not become dated and is still of value to your customers... and the search engines. Revisit your content, update it, give it a spring clean, with the objective of improving your rankings in the search engines.

**What other people say about you is more important than what you say about yourself.** Another low-cost way of getting visible in front of a larger pool of potential clients is to leverage the authority of other respected experts.

3. Focus on driving conversions

A low cost, high impact digital marketing technique to focus on is conversion rate optimisation. Small incremental changes to the user journey will turn more of your website visitors into customers.

**Social proof** and positive stories about your business form an essential part of the content on your website. Revisit how you are using your cases studies, recommendations and reviews at every touchpoint in your marketing, and take the time to weave this content throughout your website, and share actively on social media.

**Customer experience is king.** Invest in your website to ensure you are giving a fast, personalised experience. And in terms of keeping costs down, remember that small changes on your website will have an outweighed impact on the final results.

**Leverage artificial intelligence.** Now is the time to get up to speed on the latest developments in machine learning and artificial intelligence that will give
ensuring you are getting the right message to the right
drive down your cost per acquisition of new clients by
Taking advantage of current developments in AI will
the right prospective customers at the right time.
your business a competitive advantage and access to
success, and learn from the experiment.
also published, fully linked, at www.infolaw.co.uk/newsletter

also published, fully linked, at www.infolaw.co.uk/newsletter

digital marketing puzzle.
invest your cash.
works makes it easier to make the decisions of where
profitability.
explored how social media is contributing to your
before you make that decision, ensure you have
consuming and an optional non-essential activity. But
how you are going to spend your resources. One soft
option might be to put the brakes on your social media
provide to you that can shape your strategy?
Measure your social media ROI. When budgets
get tight, you may need to make tough decisions on
how you are going to spend your resources. One soft
option might be to put the brakes on your social media
activity. Social media can appear to be very time
consuming and an optional non-essential activity. But
before you make that decision, ensure you have
explored how social media is contributing to your
bottom line in terms of engagement, visibility, and
profitability.
If marketing budgets are tight, then knowing what
works makes it easier to make the decisions of where
to invest your cash.

4. Measure, measure, measure

If you don’t measure, then you can’t manage. And if
you’re not managing, then you could be pouring money
down the drain.
Measuring means accountability for your marketing
spend. You need to be measuring against your
success criteria. You may want to measure
to measure sales, numbers of lead generated, upsells, or
referrals. Now is the time to ensure you have
defined your key performance indicators.

Configure your Google Analytics
correctly. Ensure you are covering all the
basics, and you are using the data to drive
your marketing efficiencies. Do you have goals
set up correctly? Have you connected your
Search Console? Have you defined what you
are measuring? Are you taking advantage of
all the free data that Google Analytics
provides to you that can shape your strategy?

5. Test, learn, test

And finally, there is no one size fits all answer to the
digital marketing puzzle.
You will need to be nimble and creative. Measure
your success, and learn from the experiment.

• Experiments should be quick, cheap, and easy to
deliver.
• If it works, then well done, and more of the same,
please.
• And if it doesn’t work so well, then kill the
experiment and move on. No harm done. Be quick
and be ruthless. You will have tested something,
learned from it, and moving on to test something
new.

Susan Hallam MBE is Managing Director of Hallam Internet
(hallaminternet.com), a digital marketing agency helping UK
law firms to be more successful using internet technologies.
She is a Freeman of the City of London.
Email susan.hallam@hallaminternet.com.
Twitter @SusanHallam.

Divergence from EU: facial recognition

By Alex Heshmaty

It was recently reported that the European
Commission (EC) was considering a temporary ban on
the use of facial recognition technology in public places.
A draft white paper on artificial intelligence had
reportedly stated that the “use of facial recognition
technology by private or public actors in public spaces
would be prohibited for a definite period (eg three to
five years) during which a sound methodology for
assessing the impacts of this technology and possible risk
management measures could be identified and developed”.

It seems
that the EC had changed its mind by the time they
published the official white paper: On Artificial
Intelligence – A European approach to excellence and
good measure. However, in section D (f) on Specific
requirements for remote biometric identification, it
warns that: “The gathering and use of biometric data
for remote identification purposes, for instance through
deployment of facial recognition in public places, carries
specific risks for fundamental rights.” It goes on to note
that: “in accordance with the current EU data
protection rules and the Charter of Fundamental Rights,
AI can only be used for remote biometric identification
purposes [eg facial recognition] where such use is duly
justified, proportionate and subject to adequate
safeguard” and states that it will launch a “broad
European debate on the specific circumstances, if any,
which might justify such use, and on common
safeguards.” So, although there are currently no official
plans for a ban of facial recognition technology within
the EU, this is certainly a potential outcome of the
forthcoming debate.

Whilst the data protection regime in the UK is
unlikely to diverge from the EU in the short term, the
British government has suggested that there could be a
broader divergence from EU regulations (in general)
after the transition period. But in terms of automated
facial recognition, it seems the UK will not be waiting
for any European debate on the matter: the
Metropolitan Police has announced it will use live facial
recognition cameras operationally for the first time on
London streets. This announcement follows the High
Court decision in R (Bridges) v CCSWP and SSHD
[2019] EWHC 2341, the first case in the world
regarding the use of facial recognition – see Chrysilla
de Vere in INL1910.

Alex Heshmaty is technology editor for the Newsletter.
Photo by geralt on Pixabay.com.
What happens to my data?

By Chrysilla de Vere

Increasingly, the information we need and use every day is stored, accessed and controlled online. We have become accustomed to the convenience and efficiency of being able to access significant swaths of information about ourselves, our business and the world at the tap of a button.

Many of us accept that such convenience comes at a cost, with some platforms such as Facebook, Twitter and YouTube primarily being funded by advertisers. We understand that, in order to provide a free service, we must endure some form of targeted advertising, assuming this is just the same as old fashioned TV or bus stop advertising, albeit in a different form.

Every day we volunteer information about ourselves, whether by completing an online enquiry form, subscribing to social media platforms or simply by opening an app on our phone. But do we really know what happens to the information we share? Do we actually know what information we may be inadvertently revealing to others when we log on?

It appears not – at least according to a report by the UK Joint Committee of Human Rights: “The Right to Privacy (Article 8) and the Digital Revolution” (HC 122/HL Paper 14) (Report).

The Report considered how private companies’ use of personal data impacted on human rights. But its findings also revealed that “vast numbers of people are not fully aware of how their data is being used” and that the consent model used as the default legal basis for processing personal data under the General Data Protection Regulation (GDPR) is “broken”.

Companies, it seems, according to the Report, are providing the information they are required under the GDPR via a privacy notice in an overly complicated, inaccurate or vague manner.

The question posed by the Report is whether the consent we provide by ticking or checking a box is even valid under the GDPR if we do not appreciate, from the information we are provided, what is being done with our data.

Transparency

Organisations are required to process personal data only if they meet their obligations under the GDPR which include the obligation to provide data subjects with a fair processing notice under Article 13 or Article 14.

The most common form of notice is the privacy statement which is usually available on an organisation’s website or a tab in a mobile app.

The fair processing notice is designed to ensure that the data subject is adequately informed of the way in which an organisation uses their data.

Organisations must also comply with the privacy principles, the first of which is the requirement that personal data must be processed lawfully, fairly and in a transparent manner.

Fairness is not defined, but the principle is understood to refer to the effect processing has on an individual’s rights and freedoms. The ICO describes fairness as handling “data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.”

The principle of transparency requires that any information relating to processing (i.e. the privacy notice) be easily accessible, easy to understand with clear and plain language being used.

It appears from the Report’s findings, that organisations are not being transparent in their privacy notices about how they will be sharing their data, nor are they providing the notices in an easy to understand fashion.

The Report cited research by Doteveryon which found that 62 per cent of the people they spoke to were unaware that social media companies made money by selling data to third parties and 45 per cent were unaware that information they enter on websites and social media can help target advertisements (page 20 of the Report).

In a press release published by the European Commission on 13 June 2019, the results of a Eurobarometer survey on data protection, revealed that whilst Europeans were “relatively aware” of the GDPR and their rights, of the 60 per cent of those surveyed who read their privacy statements, only 13 per cent read them fully due to the statements being too long or too difficult to understand.

Similarly in the ICO’s annual report 2018/2019 the research conducted found that only one in three (34 per cent) people have high trust and confidence in companies and organisations storing and using their personal information.

Unexpected sharing of data

The Report considered the trend for businesses to share data through data brokers without the data subject’s knowledge and despite the fact that the data subject only gave consent to use of their data in return for a service from one business.

In a study conducted by Dr Binns from the University of Oxford, assessing 1 million android apps, he found that 9 out of 10 apps sent data back to Google and four out of ten apps sent data back to Facebook (page 21 of the Report).

The practice of combining data and data aggregation raised concerns about the collection of detailed profiles on individuals without their knowledge.

Most people will not be aware that information from the GPS in mobile phones or vehicles, search histories, purchases, social media posts and cookies, when combined, will create a comprehensive profile of an individual.

The Report highlighted that these profiles are being shared within “an eco-system” comprising of thousands or organisations all competing for digital advertising space through Real Time Bidding (page 22).
Real Time Bidding is a type of advertising which is in the form of an auction; companies place bids on whether they want to advertise their product to a particular demographic; eg a 21 year old male living in Reading, works in retail and likes to buy shoes.

This practice of combining your information with other data sets and being sold on to data brokers is not being explained in privacy notices.

Consumers may well not expect that their buying history with a particular website will be sold and packaged together with their IP address, browser history, political or religious views as expressed on social media.

The risk to privacy is heightened when special category data is being processed, eg internet searches on medical conditions or online purchases of medical/pharmaceutical products. Profiling of children and vulnerable people who are not as capable of understanding how their data is being used was also raised as a key concern.

Is the consent model broken?

In order for private companies to lawfully process personal data, they may rely on a number of bases under Article 6 of the GDPR, one of which is with the consent of the data subject.

For special category data which includes sensitive information such as health, sexual orientation, religion, political views, biometric information, an exemption must also be found under Article 9. One exemption that could apply is with the “explicit consent” of the data subject.

Another common basis under Article 6 is for the purpose of the legitimate interests of the organisation, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject. Often the legitimate interests of the organisation, such as the example above, to share their data with data brokers will be overridden by the “rights and freedoms” of the data subject which will prevent the processing entirely.

Because of difficulties with relying on legitimate interests and the fact that an individual’s consent can also be used for special category data, user consent is invariably being used as the default legal basis.

The challenge when relying on consent is that, to be lawful, consent must be “specific, informed, freely given and unambiguous indication given.”

If a company has failed to be transparent in their privacy notice about the proposed purposes and uses of data as required, consent can hardly be classed as informed. However, the length and complexity which may be required to adequately explain the ways in which the data is intended to be used is creating an environment where users are either not reading or not understanding the information provided.

Consent must also be freely given, which means that consent should be capable of being withdrawn at any time. The Report found that, whilst Google allows users to opt out of personalisation of ads and revoke consent, the process by which a user must go through in order to change privacy settings to a privacy friendly option was considerably longer (page 26 of the Report).

What can be done?

Privacy proponents have long called for stricter controls and specific regulation to govern the big tech firms’ use of personal data. The Government’s Online Harms White Paper released in April 2019, outlined plans for a new regulatory framework and oversight for internet companies. Some of the proposals included establishing a statutory duty of care which is enforced by an independent regulator and to ensure that companies’ terms and conditions are “sufficiently clear and accessible”, including to children and other vulnerable users.

The Report made a number of recommendations with the central theme of changing the current privacy framework.

The onus, the Committee argued, should not be on the individual, relying on their consent. Instead the government should introduce robust regulatory standards for internet companies which are rigorously enforced (page 39 of the Report). The Committee recommended that the government should explore a simpler way for individuals to see what data is being shared about them and with whom, and to prevent some or all of their data being shared at all.

Whilst it is understandable that the government sees the solution as increased regulation backed by stringent penalties, the systemic change that is needed to promote transparency will require backing of the big tech companies and a business case for it. Ultimately, it will be consumer demand for greater respect of their privacy rights that will motivate change.

Further reading

UK Joint Committee of Human Rights: The Right to Privacy (Article 8) and the Digital Revolution”


ICO: Annual report 2018/2019


Chrysilla de Vere is the Commercial partner at Clarkslegal, specialising in privacy and data protection.

Email cdevere@clarkslegal.com, Twitter @Clarkslegal.

Photos public domain from PxHere and by geralt on Needpix.com.
Divergence from EU: Copyright Directive

By Alex Heshmaty

The government recently indicated a willingness to diverge from EU regulations post-Brexit. Perhaps one of the more significant moves in this direction is the announcement by Universities and Science Minister Chris Skidmore that the UK will not implement the controversial EU Copyright Directive.

The main criticism levelled at the directive was down to Article 17* Use of protected content by online content-sharing service providers. Essentially this makes services such as YouTube and Facebook responsible for any copyright infringement contained in any content uploaded by their users to their platforms. In effect, this could potentially force platforms to substantially ramp up their efforts of moderation, resulting in huge costs associated with aggressive moderation or having to face the alternative prospect of significant fines.

Unsurprisingly, Google lobbied heavily against the proposed measures, warning that the legislation would "harm Europe’s creative and digital industries" and "change the web as we know it". Susan Wojcicki, CEO of YouTube, went as far as to suggest the consequences of Article 17 could mean that “EU residents are at risk of being cut off from” watching YouTube videos. Nevertheless, the EU is still going ahead with the directive, and EU member states will need to implement its provisions by 7 June 2021.

Since this date falls after the end of the Brexit transition period, the UK government has decided to mark one of its first major diversions from EU policy by not implementing the directive. In a written answer to a Parliamentary question regarding legislative proposals to implement the directive, Skidmore simply said that: “the United Kingdom will not be required to implement the Directive, and the Government has no plans to do so. Any future changes to the UK copyright framework will be considered as part of the usual domestic policy process”. It will be interesting to see if this position changes during the course of Brexit negotiations – watch this space!

*In the original version of the directive, Article 17 was Article 13 – and much of the debate concerning this provision refers to Article 13.

For a more comprehensive discussion of the EU Copyright Directive, see Peter Adediran in INL1907.

Alex Heshmaty is technology editor for the Newsletter.

Photo by geralt on Pixabay.com.

Bookmarks

“The abiding impression left by the government’s Initial Response to the Online Harms White Paper Consultation is that it is half-finished” says Graham Smith in Online Harms Deconstructed – the Initial Consultation Response – www.cyberleagle.com.

The Inside HMCTS Blog gives insights into how HMCTS is developing “digital justice”; see recently the post on Improving the way organisations access and manage civil, family and tribunal cases – https://insidehmcts.blog.gov.uk.

Open Info & Ideas is a new blog from Judith Townend on accessing information and the law and policy that governs it; most recently see her post on what remote court hearings mean for open justice – https://openinfoandideas.wordpress.com.

The Law Society Small Firms Division has an article by David Fleming, chief technology officer at Mitigo, with advice on cybersecurity when working from home – https://bit.ly/2QSNdAD.

Don’t wait till the end of the year to complete your CPD requirements. With our Internet for Lawyers CPD competence service you can quickly and easily create a Plan and keep the appropriate Records for SRA and BSB compliance purposes. Just Select relevant topics and you have an instant Plan and a Record which you can update as you complete activities.

Our own materials guide you through the legal resources and tools available online, help you understand the internet and the legal issues it raises and assist you in the practical application of internet services to your legal practice. You can also record other update activities.

Start your CPD 2020 plan now at infolaw.co.uk/cpd. From only £50+VAT.