Facial recognition in public spaces

By Chrysilla de Vere

Live facial recognition technology or automatic facial recognition (AFR) adds another dimension to CCTV monitoring and other surveillance methods. Using biometrics (certain physical and physiological features), the technology can map facial features to identify particular individuals by matching these with a database of known faces. This technology has been in use for some years by certain public and government agencies, but with the advent of AI and machine learning, it has become more prevalent in the private sector.

The current debate

You are walking along a side street towards your office. Unbeknown to you a closed-circuit television with facial recognition capabilities is tracking your movements. Is this lawful?

This question has recently been considered by both the UK’s Information Commissioner, Elizabeth Denham, and more recently by the High Court in R (Bridges) v CCSWP and SSHD [2019] EWHC 2341, which handed down its decision in the first case in the world regarding the use of facial recognition.

Ms Denham has also recently released statements addressing police and private use of facial recognition. She herself was an intervener in the case and indicated in July that her office was conducting an investigation into the trials undertaken by the police.

More recently on 15 August 2019 she advised that she would be investigating the use of facial recognition technology in King’s Cross London by a privately-owned development, stating that she is “deeply concerned about the growing use of facial recognition in public spaces, not only by law enforcement agencies but also increasingly by the private sector.”

The private development in question, Kings Cross Estate, has since released a statement on 2 September 2019 to confirm they had used facial recognition on the Estate until March 2018 and were co-operating with the ICO but that due to the “broad debate now under way”, had no plans to reintroduce any facial recognition technology.

Any concerns Kings Cross Estate had hoped to quell may now have been heightened by the subsequent admission on 6 September 2019 by the Metropolitan Police that they had given images to Kings Cross Estate for use with its facial recognition scheme.

An international perspective

The UK is not the only jurisdiction where facial recognition has been seen as a threat to privacy. California has recently passed a law banning state and local law enforcement from using body cameras with facial recognition. The law was backed by the American Civil Liberties Union with the bill’s sponsor, Mr Ting, citing community trust in law enforcement as the basis for the ban and that if the software was installed, it will become “a tool of surveillance which was never the goal.” San Francisco and Oakland County had previously banned use by local city agencies and police.

Unjustified surveillance by law enforcement was also a concern voiced by musicians calling for a ban on

Regulation

Alex Heshmaty of Legal Words looks at the debates around the regulation of big data companies 4

Cryptocurrencies

Alex Haffner of Fladgate explains Facebook’s Libra and considers the legal issues arising 5

Legal practice

Andrew Thornton of Erskine Chambers introduces Juriosity, the new online platform for lawyers 7

Regulation

Updates from Alex Heshmaty on digital services tax, Privacy Shield and GDPR fines 8

Websites

David Kerr and Chris Davidson of Moore Legal Technology provide the ultimate checklist for websites 10

CPD

Our Internet for Lawyers 2019 CPD competence service is online at www.infolaw.co.uk/cpd
facial recognition use at music concerts by Ticketmaster companies. Musicians have launched a campaign against such use which they say puts minority and undocumented individuals and those with criminal records at risk of being “unjustly detained, harassed or judged.”

The threat of state surveillance by facial recognition is of course heightened all the more in countries where privacy rights are limited, such as China who is a leading innovator of AI powered surveillance tools. Protesters involved in the recent Hong Kong riots feared that data captured by facial recognition systems in Hong Kong were being exported to mainland China.

This is all while Chinese companies are increasing their stake in a global market for facial recognition software with one Beijing-based company targeting an IPO raise of up to $1 billion.

**Use by private companies**

Private organisations which process personal data within the UK must comply with the General Data Protection Act (GDPR) and the Data Protection Act 2018 (DPA 2018).

Personal data is a well-recognised concept. It is data relating to a living individual who can be identified indirectly or directly from either the data collected alone or by that data and other information likely to come into the possession of the data controller.

In the *Bridges* case, the High Court found that images of members of the public caught on CCTV cameras and processed to extract biometric facial data are identified directly, or in the words of their Honours, “sufficiently individuated” to become personal data within the meaning of the DPA 1998 (para 124).

The processing of personal data must only be undertaken if any of the grounds under Article 6 of the GDPR apply. Further, where the processing involves special category data, which includes biometric data, a further justification must be found within Article 9.

**The lawful bases**

Article 6 (1) lists the lawful bases for processing. In the context of video surveillance, the applicable bases may include:

- The consent of the individuals concerned (Article 6(1)(a)). For consent to be valid under the GDPR it must be freely given, specific, informed and an unambiguous indication given prior to the processing.
- The processing is necessary for the legitimate interests pursued by the controller (Article 6(1)(f)). Processing for the purpose of “legitimate interest of a controller” will be lawful unless such interests are overridden by the fundamental rights and freedoms of an individual.

Special category data

If the processing of personal data involves special category data, in addition to identifying a lawful basis under Article 6, an exemption must also be found in Article 9 to justify such processing.

Facial recognition technology will collect a type of special category data, ie biometric data, if it is capable of uniquely identifying an individual. Biometric data involves the physical, physiological or behavioural characteristics of a person.

Therefore, if facial recognition technology is used to identify a particular individual as opposed to a category of persons (such as the profiling of customers by race, gender, age) this will be processing biometric data.

Article 9(2) of the GDPR lists a limited number of exemptions which may justify processing special category data. These grounds include the explicit consent of the data subject, vital interests of the data subject (immediate medical emergency), necessary for the establishment, exercise or defence of legal claims, processing relating to personal data already made public by the individual, substantial public interest, various medical and public health reasons, and for scientific research or statistics.

The European Data Protection Board (EDPB) recently issued draft guidelines for public consultation: Guidelines 3/2019 on processing of personal data through video devices. These specifically address the use of facial recognition technology.

The EDPB is an independent European body established under the GDPR and publishes guidance on the application of European data protection laws.

The draft guidelines make some interesting observations about the use of both CCTV and facial recognition:

1. Video surveillance may be necessary to protect the legitimate interests of a controller such as for the protection of property against burglary, theft or vandalism (para 19).

2. Video surveillance measures should only be chosen if the purpose could not reasonably be fulfilled by other means which are less intrusive to fundamental rights and freedoms (para 24).

3. It may be necessary to use video surveillance not just within the property boundaries but also in the immediate surroundings of the premises, in which case some protective measures such as blocking out or pixelating could be employed (para 27).

4. In respect of facial recognition which involves processing of special category data, the draft guidelines voice caution. The EDPB appears to suggest that for private entities that install the technology for their own purposes such as for security, explicit consent will in most cases be required (para 76).
5. Where explicit consent is required, an organisation cannot condition access to its services on consenting to the processing but must offer an alternative solution that does not involve facial recognition (para 85).

6. In cases where the technology captures passers-by, an exemption under Article 9 will still be required for these individuals (para 83). The difficulty in the case of passers-by is that if consent is relied on, this must be obtained before undertaking processing and therefore either another exemption under Article 9 must apply or such processing may be unlawful.

For organisations like Kings Cross Estate that capture the images of passers-by, they will need to find another exemption under Article 9 or risk infringing the DPA 2018.

The conclusions of the ICO’s investigation into the Kings Cross matter may provide some clarification on this point. However, if the ICO’s determination reflects the views of the EDPB (explicit consent likely to be required for facial recognition use in public), the flow-on effects for companies could be widespread. Certainly, companies which use facial recognition on individuals in public areas ought to be now reviewing their data protection compliance and procedures.

**Use by law enforcement**

As already mentioned, in the first case of its kind in the world, the High Court recently handed down its decision in the *Bridges* case. This involved the targeted employment of facial recognition in public areas on a trial basis by the South Wales Police (SWP).

The case related to a claim by a member of the public, Mr Edward Bridges a civil liberties campaigner who alleged that on two occasions he had been present and caught by the cameras in use by the South Wales Police deploying AFR software.

Mr Bridges claimed that the use of AFR by the SWP was in breach of the right to privacy as contained in Article 8 of the European Convention of Human Rights (ECHR) and that the SWP had failed to comply with the Data Protection Act 1998 and its successor, the Data Protection Act 2018 (DPA 2018). He also complained that the SWP had failed its statutory duty under the Equality Act 2010 to have regard to the possible discriminatory impacts of the technology.

The High Court found that on the facts of that case, the SWP had not unlawfully interfered with Mr Bridges’ right to privacy nor had the SWP failed to comply with the various provisions of the DPA 2018 concerning the processing of personal data by law enforcement. It also found in favour of SWP, stating that it had complied with its duty to have due regard under the Equality Act.

Some of the factors which led the Court to find that the processing was a permitted interference with Mr Bridge’s right to privacy included that the processing was undertaken in a fair and transparent manner (fair processing notices were issued and signs located close by to the camera, the police van was marked), the processing was limited in time, for a particular legitimate purpose, and biometric data which did not result in a match was immediately deleted. For further commentary on the decision, see the case analysis at [http://bit.ly/clarkslegalbridges](http://bit.ly/clarkslegalbridges).

Whilst the findings of the court are fact specific, it provided some guidance which is applicable equally to both public and private use of facial recognition:

1. The mere storing or initial gathering of biometric data is enough to interfere with an individual’s right to privacy under Article 8 of the ECHR (para 59). Apparently this view was shared by the ICO who considered that the automated capture of facial biometrics amounts to a “serious interference with privacy rights” (para 60).

2. Members of the public caught on CCTV and whose biometric facial data are taken are sufficiently identified and therefore comprise personal data for the purposes of the DPA 1998 (para 124).

3. The taking of biometric information entails sensitive processing for which cogent and robust reasons must be provided. In that regard, no distinction ought to be made between the levels of protection given in the Human Rights Act 1988 and the DPA 2018 (para 100).

4. The inclusion by police of individuals on a watch list and consequent processing of that person’s personal data without sufficient reason (ie no reasonable suspicion of having committed or about to commit an offence) would most likely amount to an unlawful interference with their Article 8 rights (para 105).

5. Whilst the court found no evidence of indirect discrimination in the particular case, it pointed out that the police may wish to conduct an investigation into whether the software may produce discriminatory impacts and pondered whether it would be appropriate for the SWP to employ a failsafe to ensure no step is taken against a member of the public unless an officer has reviewed a potential match and is satisfied there is such a match (para 156).

**Conclusions**

It is inevitable that facial recognition use will become more prevalent as technology improves notwithstanding concerns raised by privacy advocates and regulators such as the ICO.

With the global market for facial recognition predicted to grow to USD $9 billion by 2024, further clarification by the ICO and perhaps further regulation to address privacy concerns may be warranted.

Facial recognition is likely to become cheaper and more accessible as more tech companies enter the market. Use will therefore be on the rise and regulators such as the ICO in the UK and supervisory authorities within the EU are likely to reassess whether specific laws to target this technology are needed.

Companies are well advised to take a risk-averse approach to facial recognition and deploy it only where strictly necessary and proportionate to the proposed purpose. A data protection impact assessment as required by the GDPR prior to implementing the technology should assist companies assess whether their use is likely to offend privacy rights.

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

Email cdevere@clarkslegal.com, Twitter @Clarkslegal.

Image cc by Mike MacKenzie on Flickr, adapted.
The big data regulation debate

By Alex Heshmaty

Back in 2006, Sheffield mathematician Clive Humby declared “data is the new oil” after reaping the benefits of helping to set up a supermarket loyalty card scheme. This was the same year that Facebook went mainstream, accelerating the pace of data harvesting and spawning an entire industry devoted to the collection, analysis and monetisation of large sets of personal data. Although many concerns were raised over the following years regarding the potential dangers of the big data revolution which ensued, arguably it wasn’t until the Cambridge Analytica scandal broke in 2018 that the public – and their parliamentary representatives – began to grasp the true gravity of the situation.

From Big Brother to Cambridge Analytica

The exploitation of big data by business has been subject to relatively light touch regulation compared to the oversight of government surveillance. Existing Orwellian fears of democratic erosion were compounded by efforts of Edward Snowden in 2013 to expose the magnitude of digital state intrusion into personal lives. In contrast, Silicon Valley tech giants were given a free pass and were, until recently, seen more as benevolent disruptors, promoting business development and providing economic benefits for all and sundry, donning fluffy sounding taglines such as Google’s “Don’t be evil”. But some of the problematic (and probably unintended) consequences of the initial embrace of big tech – and social media in particular – have gradually become increasingly apparent, including tax avoidance, information overload, damage to the hospitality sector, and online social harms. Furthermore, collaboration of the private sector with the state sector (eg Google’s DeepMind AI being unleashed on NHS patient data) has raised eyebrows.

However, the real turning point came in the wake of a Channel 4 sting of now defunct political consulting firm Cambridge Analytica, building upon the work of investigative journalist Caroline Cadwallader. She had written an article almost a year earlier, in which she exposed the damage to democracy through the manipulation of voters via targeted advertising using the harvested Facebook data of up to 87 million people worldwide, orchestrated by Cambridge Analytica on behalf of political clients. Former Deputy Prime Minister Nick Clegg, now vice-president at Facebook, was later forced to argue that there had been no Russian interference with the Brexit vote as a result of the scandal, although there was broad consensus that it had certainly played some part in the election of Donald Trump to the White House.

Europe vs America vs China

Although the Data Protection Act 1998 (DPA) already provided certain rules pertaining to the use of big data sets, it was the introduction of the General Data Protection Regulation (GDPR) by the EU in 2018 which really set the gauntlet for big tech, providing teeth for regulating bodies such as the ICO by raising the maximum fines for data breaches to the greater of €20 million or 4 per cent of global annual turnover. The fine imposed on Facebook by the ICO for its role in Cambridge Analytica fiasco was limited to the DPA maximum of £500,000 because the breaches in question occurred before the GDPR came into effect, but more recent fines demonstrate that companies which fail to keep the personal data of European citizens safe will get more than just a slap on the wrist.

Meanwhile, privacy campaigner Max Schrems, who played a key part in replacing the Safe Harbor agreement with tighter data protection controls for the transatlantic flow of personal data in the form of Privacy Shield, continues to force EU regulators to keep a close eye on the exploitation of data by Silicon Valley. And, although not about data as such, the movement to prevent tax avoidance measures taken by big tech, seems to be driven primarily by European countries.

However, it would not be entirely accurate to frame this as simply a case of Europe trying to regulate American technology companies. Indeed a new data protection law has recently been passed in the heart of Silicon Valley: California Consumer Privacy Act 2018 AB
Facebook’s Libra under the regulatory spotlight
By Alex Haffner

“This project contains risks of abuse of dominant position, risks to sovereignty and risks for consumers and for companies” (Bruno Le Maire, French Finance Minister)

In June Facebook announced to much public fanfare that it intends to roll out a new digital currency called Libra for use in 2020, allowing its users across the globe to make online financial transactions.

It has quickly become clear that Facebook faces a significant battle to ensure that the Libra project does not become mired in regulatory and political red tape and, more damagingly still, is not able to launch across key national/regional markets. At the last count, the roll-call of those who have signalled a desire to subject Libra to careful scrutiny (as well as Mr Le Maire whose quote above makes it quite clear what he thinks) includes leaders of the G7 nations, the US Congress, the Committee on Payments and Market Infrastructure comprising representatives of 26 central banks, the European Commission and the Swiss Financial Market Supervisory Authority.

Why is Facebook Libra attracting so much critical scrutiny and what are the key issues that regulators and politicians are likely to focus on now that the project is under the public gaze?

What exactly is Libra?

According to a White Paper issued on 18 June (https://libra.org/en-US/white-paper), Libra has been created by Facebook to enable “a simple global currency and financial infrastructure that empowers billions of people.”

In technical terms, Libra will operate via the blockchain – a system on which transactions are processed and verified by independent computers rather than a single central bank or other similar guardian. This is, of course, the same technology underpinning cryptocurrencies such as Bitcoin which have attracted much debate in recent times. Unlike those currencies which are completely decentralised, meaning anyone can technically carry out processing and verification activities (subject to having sufficient computing power), these activities will only be carried out by members of the Libra Association – an “independent” not for profit body registered in Switzerland which will be formed to govern and implement the project. Declared members of the Association to date include Mastercard, Visa, PayPal, Ebay, Uber and Lyft.

Another point of difference to existing cryptocurrencies is that the value of Libra will be tied to a basket of established currencies and low-risk government securities, the value of the basket equating to Libra’s value. This is designed to avoid the wild swings in value caused by speculators in Bitcoin and other existing cryptocurrencies – their volatility means they can only be a medium of exchange in “instantaneous” transactions.
Libra users will need to open a dedicated account and digital wallet (Calibra) which will hold their Libra balance and enable them to convert “cash” (dollars, pounds sterling etc) into Libra. They can then transfer Libra to other users and make payments for goods/services from merchants who are set up to accept Libra payments. Calibra will be built directly into Facebook, as well as the WhatsApp and Instagram platforms (operated by Facebook).

**What are the legal issues?**

Since the White Paper was issued, commentators have debated how best to characterise Libra. Perhaps the best description of it is as a “mobile money” function. To that extent it is not a first in kind; mobile money offerings have become prevalent in recent times, especially following in the footsteps of the M-Pesa scheme which is widely used across Africa to “bank the un-banked”. What is different about Libra, however, is the vast consumer base immediately available to Facebook through its 2.4 billion+ registered users. Whereas other projects and schemes have generally had to build their own customer base, Facebook has the opportunity to scale immediately.

Whilst the commercial opportunity is therefore straightforward to understand, less easy to unpick are the multitudinous legal and regulatory concerns which accompany the Libra project and which are already exercising global supervisory and governmental bodies. These can best be summarised as follows.

**Licensing**

Payment services are carefully regulated across different jurisdictions. In some instances, providers can “passport” licences obtained in one jurisdiction to be able to provide the same services elsewhere – notably the case with the EU. Nevertheless, given its global reach, Libra will potentially be subject to a whole patchwork of licensing and regulatory regimes.

Particularly relevant in this context is the extent to which Libra may be regarded as more than a payment service provider and more akin to a banking provider. For example, users’ ability to deposit and withdraw funds from their Libra “account” suggest the service will operate like a traditional bank account (and indeed much of the fuss around Libra appears to centre on whether Facebook is in effect seeking to circumvent the existing banking model). Banks are, for obvious reasons, traditionally, more heavily regulated and subject to more onerous licensing requirements than payments providers.

It is instructive in this regard that a recent guidance note from the Swiss Financial Markets Supervisory Authority (FINMA), ostensibly dealing with the regulation of Initial Coin Offerings (ICOs), reported on FINMA’s preliminary assessment of the regulatory position regarding the Libra Association. In particular, FINMA observed that, as well as requiring a payment system licence, additional prudential requirements are expected to apply as it will provide more than just a pure payment service. Notably, FINMA declared that it would adopt a “same risk, same rules” approach to ensure that, should the Libra model give rise to typical banking risks, it will apply banking regulations to the project. Specific mention was made of the intended Libra reserve (ie the mechanism by which the currency’s value will be pegged) and the need to ensure that any risks arising from the management of that reserve are borne entirely by the currency issuer, not the currency holders.

**Risk management**

Facebook has (understandably) sought to create a clear distinction between Libra and existing cryptocurrencies which have attracted much negative press given the difficulty in tracing those who trade in them and the systematic risks involved in any global trade of crypto.

In many ways, Facebook’s ability to readily create a digital identity for users of Libra (who likely will already be users of existing Facebook services) is therefore a major positive when compared with other decentralised/blockchain based services. However, Facebook’s aspirations appear to go further than simply cross-selling another service to its existing user-base in developed economies. The White Paper talks, for example, about targeting the “unbanked” in developing economies – how to ensure those users can be readily identified and checked is less obvious, given they likely will not have identity documentation traditionally used for due diligence purposes.

Some commentators have already posited the theory that, if it achieves its ambitions in terms of traction and usage, Facebook will become more powerful than central banks in developing countries in its ability to control monetary policy. This in turn raises important questions about whether a private consortium is better placed than the banks to manage money flows in such countries.

**Data protection**

As ever with “big tech” and particularly Facebook, data protection concerns are never far from the surface.

It is self-evident that Facebook intends to leverage its existing client base to “sell-in” the Libra service. Given previous misdemeanours with regards to customer data (including the Cambridge Analytica scandal for one), close attention will be paid to how Facebook intends to deal with customer data as part of this project.

With such concerns in mind, Facebook has already emphasised that Calibra (ie the operator of users digital wallets) will operate as a standalone regulated
subsidiary so as to ensure a separation of social and financial data. However, one would expect that regulators will want to get more concrete assurances that any “mixing” of data will only take place with consumers’ prior consent and subject to appropriate safeguards as to storage etc.

**Competition law**

A final, battlefront for Facebook in its pursuit of the Libra project is the scrutiny which it has attracted from competition law/antitrust regulators. To that end, the EU Commission recently announced a formal investigation under its competition law powers into Libra, issuing a questionnaire to interested parties which cited “possible competition restrictions” on information exchanged as between participants in the Libra Association and their use of consumer data, indicating that there are concerns in particular as to Facebook’s ability to drive out competitors who may wish to offer similar services.

The EU Commission’s investigation feeds into a broader debate, already raging across the pond in the US, as to Facebook’s market position and ability to leverage the market power it exercises in social media and digital advertising to the detriment of consumers. It was confirmed by Facebook in July of this year that the US Federal Trade Commission had opened a probe into the company’s prior acquisitions and their impact on competition in social media, digital advertising and mobile applications. It seems likely that, as part of their investigations, the FTC will consider how the Libra project might further impact on the competitive dynamic of those markets.

**Next steps**

The Libra project itself is fascinating on many levels. From a regulatory perspective it undoubtedly poses questions which are without any obvious precedent given that, to date, most regulators have tended to keep more of a watching brief on the burgeoning market for cryptocurrency. Arguably, the fact Facebook with its global reach and user base has become involved will now hasten those regulators’ need to clarify their thinking.

For its part, Facebook has already confirmed it intends to engage closely with appropriate regulatory authorities, effectively throwing down the gauntlet to them to set out precisely what they expect the company to do to remain compliant. Likely once it gets a sense of those requirements, Facebook will need to decide whether it is willing to bear the burden of meeting regulators’ varying requests.

In the meantime, one can expect other interested parties to try to take advantage of the regulatory uncertainty to which Facebook is currently subject. Just last month, it was revealed that China is close to unveiling its own cryptocurrency through the People’s Bank of China which will be fully compliant with all local laws on money laundering and fraud.

---

Alex Haffner is a partner in the corporate department at Fladgate (www.fladgate.com). He specialises in competition, regulatory and commercial law matters.

Email ahaffner@fladgate.com. Twitter @fladgatelp.

Image cc by BTC Keychain on Flickr.

---

**Juriosity: building a legal marketplace**

*By Andrew Thornton*  
Juriosity.com was launched in partnership with the Bar Council of England and Wales in 2018. In its current form, the platform provides a directory of practising barristers and other legal professionals and a self-publishing platform enabling barristers (and other approved contributors) to publish short articles on legal developments, cases they have been involved in (or wish to comment on) and any other topics they believe will be of interest to their clients and potential clients.

Phase two of the development of Juriosity will add direct access functionality and a marketplace for the purchase and sale of precedents, contracts, guides and other collateral.

**Starting with the Bar**

In launching Juriosity, we realised that we face a bit of a “chicken and egg” issue. In order for any online marketplace to work, it has to have both sides of the transaction represented. Thus, in Juriosity’s case, it requires both lawyers and clients in order to make it a success.

We decided that the best way to approach this was to try and get as many barristers onto the platform as possible and were really happy to agree a partnership with the Bar Council. As a result, on renewing their annual practice certificates, barristers are given the opportunity to join the Juriosity platform and the vast majority do. Over 6,000 barristers and most Chambers have gone on to augment their profiles with further information about them and/or their practice.

That has given us the confidence to proceed with phase two of Juriosity’s development. Accordingly, as well as seeking to expend the offering to solicitors, we are trialling a triaged direct instruction service with three leading barristers chambers through our sister company, Sparqa Legal, with a view to launching our fully automated direct access functionality as well as a document purchase marketplace during 2020.

There are broadly two types of user on Juriosity. Those that add content and those that consume the content. The former includes barristers and solicitors who are entitled to add content provided they hold a valid practising certificate. Others who might want to add content (eg academics and others) can be given contributor status by individual application.

Content can be consumed by anyone interested in it by mere registration on the platform.

**The technology context**

Technology has significantly changed the way in which lawyers carry out their practices. Legal research has ceased to be a chargeable item for law firms and a number of them have launched on-demand, fee-earner arms and/or moved teams to non-traditional locations with a view to reducing their fixed costs and taking advantage of IT developments. The development of AI or big data tools is fundamentally changing the way in which law firms approach document heavy tasks such as disclosure, due diligence and drafting. Algorithms
provide reliable alternatives to human resource at a fraction of the cost. Firms are having to rethink their cost structures and to embrace technology (some engaging software specialists at a senior level or investing in start-ups).

The Bar has moved a bit slower. This is unsurprising with the management structure of a chambers (often one member one vote) not naturally suited to rapid change. Thus, although barristers can now accept instructions on a direct access structure or set themselves up as partnerships, the Bar is only just starting out in looking at how those developments could provide significant market opportunity.

One thing that has not materially changed is how clients find and instruct lawyers. It is true that an online directory might be used instead of the Yellow Pages but the nature of the interactions between client and lawyer has not really evolved. Law firms and barristers still tend to find their work in the same ways they did 20 years ago.

When looked at in the context of the broader economy, this is surprising. Consumers are comfortable sourcing goods and services online. Online marketplaces have made it possible to source products and services from a much broader set of sellers than ever before giving the consumer the power to buy what they want at the best price. If a consumer wants to work out which drill is most suitable for their needs, they are many sites that will help. If people are willing to buy goods online, why would they not also source legal advice in the same way?

**An online marketplace for law**

An online marketplace for accessing law and lawyers is a natural (and we think inevitable) development. It offers too many advantages not to emerge, both for consumer and lawyer.

For the consumer, it should increase access to justice. Technology ought to make it possible for anyone requiring legal assistance to find the right lawyer and/or the right legal information at the right time and at the right cost. At the moment, while a large corporate client has no difficulty in accessing the law and has the firepower to negotiate fees, the same cannot be said for a small business or a consumer who will struggle to ascertain who is the right person for the work required and will have little information about fee rates or any real ability to negotiate them.

The risks for a consumer are not as great as they might be when buying other goods and services online. Many of the issues arising when buying online are reduced or eliminated when accessing legal advice given that it is a regulated industry with professional bodies to complain to when the service provided is inadequate.

A legal access platform will assist lawyers in marketing their businesses. Just as consumers find it difficult to identify the right lawyer to use, lawyers find it difficult to market effectively to consumers. Too much is left to chance and lawyers are faced with scatter-gun marketing or restricting their business to existing clients, recommendations or clients located geographically close to them.

The opportunity for lawyers to adopt flexible working practices will be enhanced by a direct access platform. In due course there is no reason why freelance lawyers should not become a reality, able to pick and choose when they work so as to fit in with their other commitments whether family or other.

Adding marketplace functionality to the platform enabling consumers and businesses to access contracts, legal guidance, check-lists and other collateral will also enhance access to the law and reduce the amount of duplication that can arise in the current market. There is no reason why multiple clients should pay significant amounts for simple legal documents that are deployed over and again. Simple legal documents should be accessible from an online marketplace with the intervention of a lawyer only necessary in less simple situations or where a client wants the reassurance of speaking to a human.

Such a marketplace should also provide additional revenue opportunities for lawyers. No longer will lawyers only monetise their knowledge when they receive specific instructions from a client in specific circumstances. Lawyers will be able to create products (think standard form contracts, pleadings, how-to-guides) and receive a payment each time a client downloads them.

Finally, the development of open banking is going to change the relationship between a bank and its customers with banks wanting to offer a range of additional non-banking services to their core offerings with a view to increasing customer loyalty. An obvious route for banks to take is to offer legal services or introductions to legal services via their digital client platforms. Thus, in the future, a customer of a bank may simply select a lawyer through their banking app. That creates incredible opportunity for disruptive entrants to the legal market.

Andrew Thornton is a member of Erskine Chambers and a director of FromCounsel.com, Sparqa.com and Juriosity.com. Email athornton@erskinechambers.com, Twitter @juriosity.

**New digital services tax implemented in France**

Governments around the world have grappled with the challenge of sufficiently taxing international companies – particularly peripatetic tech giants - which aggressively pursue policies of (perfectly legal) tax avoidance. One of the main reasons that so many Silicon Valley icons decide to base their European operations in Dublin (including Google and Apple) is due to the low rate of corporation tax in Ireland (compared to most other EU countries) – and the ability to further minimise their taxes by taking advantage of tricks such as profit shifting. The G7 have been discussing the best way to implement a fair method of...
international taxation - but, in the meantime, France has decided to go ahead and impose its own levy, to the consternation of the US.

The French Senate approved a new law in July 2019 which levies a 3 per cent tax on digital services gross revenue (as opposed to profits) made in France by companies with total worldwide revenues of more than €750 million – of which at least €25 million is generated in France. Dubbed the GAFA tax (after Google, Apple, Facebook, Amazon), it applies retroactively from 1 January 2019 and is estimated to affect around 30 companies.

Donald Trump initially ordered an investigation into the new tax, raising fears that this could spark a trade war. But following G7 talks, Emmanuel Macron announced that an international agreement was finally in sight – “On the digital tax we have reached a deal to get beyond the difficulties we had between us” – and that the GAFA tax will be scrapped once this has been implemented.

The UK has also announced plans to introduce its own digital services tax in 2020 which would apply a 2 per cent levy on the revenues of search engines, social media platforms and online marketplaces. But whether or not this will actually make it onto the statute books before the aforementioned international tax is implemented – especially in light of legislative delays caused by Brexit – stands to be seen. – Alex Heshmaty

First GDPR level fines in the UK

One of the key changes brought about by the General Data Protection Regulation (GDPR), which came into force on 25 May 2018, was a substantial increase in the maximum fines available for data protection breaches, to the higher of £20 million or 4 per cent of global annual turnover. Any breaches which occurred prior to this date were subject to a maximum of £500,000 set by the Data Protection Act 1998 – and this former upper limit was only invoked once, in the case of Facebook and its part in the Cambridge Analytica scandal. Many commentators pointed out that half a million pounds was “chump change” for the tech giants. The same couldn’t be said of the £183 million fine which the Information Commissioner’s Office (ICO) levied on British Airways (BA) less than a year later.

According to the ICO, a malicious hack of BA’s website began in June 2018 (ie after the GDPR came into force) and led to the personal details of some 500,000 passengers being compromised, including names, emails and credit card information. The record breaking fine amounts to 1.5 per cent of the worldwide turnover of BA in 2017 – so it could have potentially been a lot higher. It has been reported that BA will appeal the fine.

Following the announcement of the BA fine, the ICO took another bite out of corporate profits with its new teeth the very next day, proposing a £99.2 million fine for the international hotel group Marriott as a consequence of a data breach in which cyberattackers stole the records of around 339 million guests.

These GDPR level fines, rather than being merely being symbolic, are probably a sign of things to come. Companies which have hitherto paid lip service to cybersecurity – particularly those which process vast amounts of personal information – need to sit up and take note of the ICO’s new armoury. – Alex Heshmaty

Max Schrems: the return

In the wake of growing data protection concerns around the turn of the century, a framework dubbed “Safe Harbor” was agreed between the EU and the US in 2000, which essentially permitted transatlantic free-flow of personal data.

Towards the end of 2015, as a result of one of several legal challenges brought by prolific Austrian privacy campaigner Max Schrems, the European Court of Justice declared the Safe Harbor framework invalid on the grounds that it did not provide adequate safeguards for personal data.

Following the landmark judgment, the relevant data protection bodies hurriedly created a replacement framework which was adopted by the European Commission in July 2016 - the EU-US Privacy Shield. This purportedly beefed up protections for the personal data of EU citizens, tightened safeguards and introduced more effective methods of redress for individuals.

But the tenacious Herr Schrems has lodged a fresh legal challenge over standard contractual clauses, which companies use to transfer customer data between their various geographical hubs. Although not a direct challenge to Privacy Shield, it has been reported that a court hearing in July 2019 asked a series of questions about the legality of the replacement framework.

Furthermore, it is understood that a separate hearing on Privacy Shield was recently postponed to await the outcome of the case on standard contractual clauses.

Commenting, Mac Schrems said: “There is fundamentally a clash between surveillance laws in the US and privacy rules in Europe ... We’re in a debate about who governs the internet. Europe governs privacy, but the US governs surveillance.” – Alex Heshmaty
The ultimate law firm website checklist

By David Kerr and Chris Davidson

It's all about the first impression. For most potential clients, your website is your shopfront. Does it belong on Oxford street or skid row? This guide will help you find out.

Step 1 – Google your firm

The first step is to search for your firm in Google (I'm sure you don't need a step-by-step on this!) both on your laptop or desktop PC and on a mobile device. If you have a tablet and a smartphone, then search from both devices as rankings and user experience can be very different from device to device. This lets you see how your site is presenting to users when they search for you. While we're probably well used to seeing this page and thus take certain elements of it for granted, however many elements can be manipulated to a certain extent. The effect of this is to create a more favourable impression in the mind of potential clients.

Anatomy of a search engine results page

Below is an example of a result from a Search Engine Results Page for a hypothetical firm which we've annotated to explain its key features.

1) The Google “Knowledge Graph”.

This section aims to provide factual information about people, places and things, right within Google. What’s within the box can dramatically vary based on the type of search carried out (ie navigational or transactional) or what is being searched for (a law firm, a movie and a person will all yield different results).

In this instance, we can see images of the office and a map listing, reviews, opening hours and so on – these are broken down into more detail below.

2) Your firm’s name and reviews.

It's worth checking to see if the name is correct and formatted correctly (you'd be surprised...) and (perhaps most importantly) that reviews are present and positive. Having positive reviews appear here and next to your main results improves “click-through rate”, ie the number of people who click through to your site from search. You can download our Google review template here.

3) Map Pin.

Make sure that your firm has a Google “my business” listing and is shown on the map. Anyone visiting your office for the first time is likely to use this to find you, so it pays to keep it right! It also pays to make sure that the “See outside” image is accurate – Google often shows a less than flattering view!

4) Your firm’s address and opening hours.

Check that the address is correct (again, you'd be
surprised...), that the opening hours are correct and that the telephone number is correct.

5) Reviews from other sources. As mentioned above, Google will pull information from other sources. In this case, it has pulled through Facebook and Yell reviews which have been sought as part of this firm’s overall strategy.

6) Reviews themselves. Google will pull through the text of reviews (good and bad!) to give users an idea of what your firm is like. We mentioned above that you can “manipulate” search results to a certain extent but with bad reviews, prevention is far, far, better than cure. Once a bad review is up it can be hard to remove.

7) People also search for. This shows other businesses people who have visited your site have searched for. This gives you an insight into who your clients think your competitors are, and it lets you check their online activity out!

8) Google Ads. This is a “pay per click” Ad targeted at this firm’s brand name. While this may seem counterproductive, it allows them to own a piece of key SERP “real estate”, builds trust in the user and, as a result, increases click-through rates.

9) The number one spot. The most sought-after position in digital marketing. While you *should* appear first for your brand name, it’s possible that you may not. We have, for instance, come across law firms who are pushed into position 2, 3 or further down for searches relating to their brand because of news reports mentioning them, similarly-named businesses in other areas (one client of ours vies for position with a footwear brand and a restaurant in some searches!)

There are three elements here: the URL, which should take care of itself, unless you’ve moved your site recently, the title (here in blue) which should be your firm’s name and the short description. The description should be succinct and capture what you do and where you do it.

10) Related pages. If your page is set up correctly, then the related information should pull through automatically. This can include your best or most popular pages. As you can see, this snags you a whole chunk of prime Google real estate.

11) Second organic result. In this case, it’s the firm’s Facebook page. As you can see, this firm has proactively sought 5-star reviews which show here and in the next three results.

13) More organic results. This time, a directory listing. It pays to check if these are present as they send powerful signals to Google about your domain.

Step 2 – Google yourself (and others)

The next step is to carry out a Google search for your name (add the word “solicitor” or “lawyer” if you need to narrow it down. Check what appears. Your bio on the firm’s website? Great (provided it’s up to date and accurate!). Your LinkedIn? Great, with the same caveat as above. Your Facebook or Twitter? Again, great if they are appropriate for professional consumption! What about articles you’ve written, cases you’ve been involved in and so on?

Do the same exercise for some of your colleagues. There’s a fair chance that anyone who has instructed you in the past will do this (individual bios are *always* among the most viewed pages on a site) and check things as are good as they can be, in line with the above.

Step 3 – Sweep your site

Now on to your website itself. A critical examination of function, design, layout and ease of use (from a potential client’s perspective) can unveil all sorts of quick-win improvements. It can be easy to get caught up in the “look and feel” of the homepage based on instinct, but we’re going to go a little deeper.

Start with the homepage but also open a sample of other pages including your blog, the main people page, some sample bios, a service page (ie your Wills page), your testimonials/reviews page and the Contact page.

Here’s what you should be looking for:

Readability and accessibility

Does your website load quickly?

PageSpeed is a ranking factor in Google; people have less patience now than ever before, so a slow site is a sure way to lose potential clients.

Is the text legible, easy to read and well-spaced?

While the colour scheme and layout might seem stylish, it must still be easy to ready on a variety of devices for the majority of people. Is there sufficient contrast between text and background?

Are there add-ons - and are they working?

Times have changed, but there was a fashion a few years ago to have all sorts of bells and whistles. If your site still has Flash plugins or other functionality which requires time to load, people are likely to leave. Particularly if they don’t work or look dated

Are your images correctly tagged?

A good website will have the images tagged with an appropriate name which make sense to users and Search Engines alike. Visually impaired visitors will use these tags to understand the image, and so will Google. To find out if your images are tagged, right click and click “save as” (don’t actually save it though). The name your PC attempts to use is the “tag”. If it says something like “img1.jpeg” rather than, say “Divorce Lawyer Birmingham”, then it should (ideally) be changed.

Branding, identity and trustworthiness

The first question a potential client will ask is “who are you?”, “can I trust you?”, then “can you do what I need?” It’s vital these questions are answered quickly. If you suspect that people are leaving the site quickly, you can check your “bounce rate” in Google Analytics.

Your logo

Is it prominently placed in the top left? Is it sufficiently high-resolution?

Your tagline

Is it prominent, obvious and does it neatly encapsulate what you do and what your USP is?

The 5-second rule

Web designers talk of the “5-second rule” - that is, you have 5 seconds to make a great first impression. In reality, it’s probably closer to 2.1 seconds but web users are fickle, and you need to get your message
across quickly. Can you understand what your firm is about within 5 seconds of viewing the homepage?

**Calls to action**
Are there prominent calls to action in key positions?
Is the telephone number displayed prominently without the user having to scroll down? Can you see a Contact page? Is there a clear prompt to the user to take action, eg “call us now”, “read more”, “click here” etc?
Is there a contact form?

**Are staff bios in place? Are photos current?**
This is a critical component of trustworthiness - people pages. These are almost always the second port of call for users, after the page which relates to the service they need.

**Navigation and structure**
Once people have formed an impression of who you are and what you (and hopefully stayed on the site!) they will begin to navigate the site. The question is can they do so easily?

**Is your main navigation easily identifiable?**
Can users find your main menu (or menus) quickly and easily? Is it easily readable?

**Is it laid out in a way that makes sense?**
One of the main criticisms we have of many law firm websites is that they are laid in a way that reflects the firm’s structure, rather than according to what users want. Does your navigation lead the user down a path to find the right solution for them, or does it simply present your practice areas in a list?

**How many different menu items are there?**
How many levels of navigation are there? If you are getting past seven menu items and have more than two levels of menus dropping down, it’s time for a rethink.

**Usability and functionality**

**Does your logo link to the home page?**
A small thing, but one users will expect.

**Are links easily identified?**
Is it obvious which words in the text are linked? Are there an appropriate number? Does every link use appropriate text (ideally, the link should be eg “divorce lawyers” not “click here”)

**Do all links work?**
An important one for both user experience and search engines. If links return a “404 page not found” error, then immediate remedial action should be taken as this is harming your site. You don’t have to manually click every link – a tool like Screaming Frog (free and paid versions available) can do this for you.

**Content**
You’ve heard it before – content is king – and we want our kingdom to be consistent, organised, easy to skim through and to meet Google’s various guidelines.

**Are headings clear, distinctive and optimised?**
Most people will simply skim read online. Ensure your headings stand out and use phrases similar or identical to the keywords you want to rank for.

**Are colours and fonts consistent?**
Fairly self-explanatory, but make sure all pages have a consistent look and fee.

**Is it in-depth, on-brand, clear and explanatory?**

Does it comply with Google’s guidelines concerning being in depth (700–1,200 words is optimal) and expertly written (correct and free from typos)?

**Are page titles explanatory?**
Does the little title which appears in the browser tab reflect the content of the page? It should be succinct, contain keywords without being spammy and closely reflects the page content.

**Are URLs meaningful and user-friendly?**
There’s debate about the usefulness of having keywords in URLs, but making sure they are readable by people is generally good practice. Having www.yoursite.co.uk/family-law is preferable to having www.yoursite.co.uk/article/030200-1303092,00.html

**Is your blog up to date?**
Has new content been added? Does the content which has been added reflect your firm’s overall strategy?

**Step 4 - Check your rankings**
While rankings are important, they are only one part of the mix. Rankings can vary from search to search based on your browser history, location, type of device and so on. It’s also important to remember the “long tail” of rankings – we all want our site to rank for our main keyword (Criminal Lawyers Liverpool, for example) a well set up site will rank for myriad other combinations of keywords such as questions. Often these are more transactional in nature and thus more desirable.

That caveat aside, it’s relatively easy to check your rankings. You can, of course, simply Google your chosen keyword and note where you rank. However, as above, your browser history or location can affect this. For instance, a search for “best Italian restaurant” will show a selection of eateries near you, not the restaurant objectively regarded as the best Italian in the world. (Google assumes you’re hungry and looking to eat, rather than carrying out research!)

There are some useful tools to assist with checking rankings. Some allow you to check rankings on the fly, some to check them in bulk, and others even to track them over time (see [http://bit.ly/moorechecklist2](http://bit.ly/moorechecklist2)). It’s important to understand what you want to rank for. It’s relatively straightforward to get a site to rank for a very specific keyword which won’t generate traffic - they key is to ensure that the keywords you choose are desirable and profitable. The tool AnswerThePublic gives an insight into the type of things people are searching for.

**Further steps**
Further steps you should take include: 5) Check how the site has performed over time with your site’s Google Analytics; and 6) Think about what else you could be doing – eg what would you expect to see in other industries or when you are researching a purchase?


David Kerr and Chris Davidson are directors at Moore Legal Technology. Email chris@moorelegaltechnology.co.uk or david@moorelegaltechnology.co.uk. Twitter @Moore_Legal.