Getting cookie consent right

By Eduardo Ustaran

One could be forgiven for thinking that knowing how to comply with a legal obligation that has been in place for nearly a decade would be clear cut. However, widespread practice tells us that this is far from the truth. In November 2009, as part of wider reforms to the European telecommunications regulatory framework, the European Union introduced various amendments to the existing Directive 2002/58/EC (e-Privacy Directive), including to the provisions regulating the use of cookies.

Since then the e-Privacy Directive has required obtaining the consent of users in order to store or access information (typically cookies or similar tracking technologies) on their devices. The only exemptions to this requirement are where this is for the sole purpose of transmitting a communication or where it is strictly necessary to provide an internet service explicitly requested by the user (see http://bit.ly/e-privacydir).

In May 2011, the UK became the first EU Member State to implement this obligation into national law. Other countries have been following suit ever since. Over the years, regulatory authorities have been providing guidance about how to comply with the cookie consent obligation in practice. In 2013, the Article 29 Working Party provided a pan-European view on this issue (http://bit.ly/e-privacydir2). They argued that a website operator wishing to comply with the e-Privacy regime would need to implement a mechanism including some key elements, namely:

- specific information,
- prior consent,
- indication of wishes expressed by the user’s active behaviour, and
- ability to choose freely.

In 2018, the General Data Protection Regulation (GDPR) introduced a strengthened concept of consent, which by effect of EU data protection law, is applicable to the consent required under the e-Privacy Directive. The GDPR stresses that consent should amount to an unambiguous indication of wishes expressed by active behaviour. To reiterate this point, the Court of Justice of the European Union (CJEU) set out in its Planet49 decision of October 2019 some key aspects applicable to the cookie consent obligation (http://bit.ly/curia-planet49), namely:

- Consent must be active, rather than passive.
- Consent must be unambiguous. According to the CJEU, “only active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement.”
- Simply giving users the chance to opt out by un-checking a pre-checked box does not constitute valid consent since “consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of the website user.”
- Consent must be specific. This means that “it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject’s wishes for other purposes.”

How do current practices fare against these requirements?

Against this background, websites have adopted different types of mechanisms aimed at meeting the cookie consent requirement. Here are some of the most commonly adopted approaches and how they fare against the standards required by law as interpreted by the courts.
Notice only approach

This website uses cookies to improve your experience. Find out more.

Some websites simply provide a very brief notice and ignore the consent requirement altogether. In some cases it may be possible to opt-out of cookies by changing the settings.

Verdict: Non-compliant.

Consent assumed from use of a website

We've placed cookies on your device to help make this website better. By continuing to use the site we assume you consent to this.

This approach acknowledges that the website operator has already placed cookies on the device and an assumption is made that the user will accept this. Not only there is no specific action to provide consent, but cookies are dropped by default.

Verdict: Non-compliant.

Consent implied from user's other actions

We use cookies to give you the best online experience. By accessing the website you give your consent to our use of cookies.

Historically, this has been one of the most common approaches to cookie consent because in the past, regulators have suggested that it might be possible to imply the user’s consent from their actions when this was specifically brought to their attention. However, even if the placing of cookies is suspended until the user takes any further action (such as clicking on a link), this practice fails the Planet49 decision test that consent must be specific and not simply inferred from actions taken for other purposes.

Verdict: Non-compliant.

Mixture of implied consent with affirmative action

We use cookies to improve and personalise your experience. By continuing to use the site, you agree to our use of cookies. [AGREE]

Some websites appear to be transitioning from the implied consent approach without completely abandoning it. The wording of the banner states that the use of the site amounts to consent, but it also includes an “Agree” button. Retaining implied consent makes this approach inconsistent with the Planet49 decision.

Verdict: Non-compliant.

Cookie wall or barrier page

To access our site you must agree to our use cookies as explained in our Cookies Policy. [PROCEED]

Some websites present the user with a banner that prevents access to any content until the user has agreed to proceed on that basis. In this situation, there is no doubt that the user must take affirmative action to specifically consent to cookies. This approach will meet the Planet49 decision test but potentially faces the challenge of no complying with the “freely given” requirement.

Verdict: Arguably compliant, as long as the regulators and courts accept a “take it or leave” approach to cookie consent compliance.

Single “Accept” button

We use cookies to deliver our online services as set out in our Cookies Policy. To consent to our use of cookies, click Accept. [ACCEPT]

This approach simply requires users to click on an “Agree” or “Accept” button for any non-exempt cookies to be used. For this practice to be compliant, such cookies can only be deployed once the user has clicked on the button.

Verdict: Compliant.

Choice of accepting or rejecting cookies

This website uses cookies to improve the quality of our website. You can accept or reject cookies by clicking on the buttons. [ACCEPT] [REJECT]

By providing a choice between accepting or rejecting non-exempt cookies, this provides a best-practice approach to cookie consent compliance.

Verdict: Compliant and best practice.

Internet Newsletter for Lawyers is edited by Nick Holmes and published by infolaw Limited
ISSN 2046-9284. Personal Print+PDF subscription (6 issues) £50. Personal PDF £30+VAT. 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
Online Court” were soon endorsed by Lord Briggs in his *Civil Courts Structure Review* and in 2016 in a joint statement by the Lord Chancellor, Lord Chief Justice and Senior President of Tribunals “Transforming our Justice System” which kicked off the courts reform programme currently being pursued by HMCTS.

Susskind argues that we should deploy technology to transform processes rather than simply to automate and improve existing ones. His model is an extended court service comprising three tiers through which cases escalate:

1. Dispute avoidance. Assessment/triage via online guidance to establish whether there is a justiciable grievance – a mix of private and government provision.
2. Dispute containment. Facilitation by case officers working with the parties in settling disputes; not an alternative but an integral part of the process.
3. Dispute resolution. Asynchronous online judging, essentially deciding cases “on the papers alone”. This could mirror existing processes, but moving away from the adversarial model, judges could take “an inquisitorial, problem-solving approach” as in civil law jurisdictions.

The vast majority of cases do not require their day in court.

In Part III he answers the wide range of criticisms ranged against online courts, including that they will be inferior to their bricks and mortar counterparts, that they will lack transparency, not deliver a fair trial and be inferior to their bricks and mortar counterparts, including that they will lack transparency, not deliver a fair trial and be inferior to their bricks and mortar counterparts.

In Part IV he looks (briefly) to the future – virtual reality, AI, robo-judges and all. None of these technologies is important to his argument but give a taste of what could be.

His concluding chapter is a powerful call to arms. “If their promise is fulfilled, ... then the social good that is public dispute resolution will be much more widely distributed across society”. Online courts can bridge “the enormous gulf between knowing ones rights and being able to enforce them” in which space the corrupt, the unsavoury and the powerful have been able to pursue their own ends, and they “will surely change behaviour of those who might otherwise be inclined to disregard the law”.

Nearly half the world’s population live without the protection of the rule of law and in Brazil there is a backlog of 100 million cases waiting for court. Susskind asks us to get behind a program to roll out his vision for online courts globally via a standard, adaptable, global platform.

This is an ambitious goal. How will we get there? Come back in four years to find out!

---

**Online Courts and the Future of Justice**

Reviewed by Nick Holmes

Four years on and Professor Richard Susskind has written the same book he wrote last time, so he says. He jests, yet again. The message and the underlying arguments remain constant; the same analogies are deployed (you know, the drill); but tech has moved on, more is feasible and the vision is developed and refined accordingly. His previous works have covered wide ground: law, lawyers, professions. The narrower focus of this work enables him to treat us to a more extensive, deeper consideration of the subject.

This is not a book about legal technology but an argument for repurposing the justice system to serve more people, employing technologies that are already well established and replacing cumbersome procedures that leave too many denied the justice they deserve.

In Part I Susskind examines the philosophical questions: Why do courts matter? What is a court? and What do we mean by justice and access to justice?

There is some fuzziness around the term “online courts” which can be taken to mean many things. Principally, it may refer to online judging or extended online court services. Richard explores it in both senses.

In considering ways to improve access to justice we should extend our concept of the delivery of justice beyond the resolution of disputes (through court processes) to the containment of disputes (through processes such as ADR) and the avoidance of disputes (through a wider understanding of the law), even to “legal health promotion” (affording access to the opportunities the law creates).

In Part II he sets out his vision for how this will be achieved. This builds on the vision first articulated in the February 2015 report for the ODR Advisory Group which he chaired – *Online Dispute for Low Value Civil Claims*. The recommendations for establishing “HM
Optimising your images to rank well

By Susan Hallam

The way in which we search for images is evolving and changing, and Google has announced that image search is a big topic in the search engine optimisation community.

Once upon a time we would search for images primarily for the purpose of copying and pasting an appropriate image into our presentations or documents. We were using image search as a source of stock photography.

But today, searchers are using image search for more than just stock images. We are using search as part of our buying process or to help us learn something new or to achieve a goal.

Our intention using image search has changed. As a result, you will need to change the way you are optimising your images in order to ensure your images are getting in front of the right eyeballs and driving the traffic you need.

So, what steps do you need to take to optimise your images for SEO?

First, check to see what images from your site that Google is already indexing. Go to Google’s Image Search (https://images.google.com) and in the search box type in site:www.yourdomain.co.uk. Google will display all the images from your site in the index.

What you’re checking for is that all of your images are indeed being crawled and that they have a chance to be ranking in the search results.

You can also add a keyword to the search to see if particular kinds of images are indexed. For example, in the search results pictured below I included the word “award” in addition to the site command.

How to optimise your images for the search engines

Following are the steps you need to take to optimise your images.

1. Give your image a keyword-rich file name

If you have a picture of a blue widget on your site, then name the image file blue-widget.jpg. Consider putting dashes between the keywords in the file name, for example, the featured image is named Image-search-Optimising-images-for-search.jpg.

2. Use an image format that Google indexes

Google only considers the following formats to be images: JPEG, GIF, PNG, BMP, and SVG as well as newer image formats like JPEG-XR and WebP. We recommend using either JPEG, GIF or PNG as these are best for optimisation. The JPEG format are most commonly supported and can keep the file size down.

3. Use the ALT tag effectively

Adding a descriptive text to the “alternative text” field for the images on your website helps to tell the search engines what your picture is about and will help you rank better in the search results. The alt tag needs to contain the key phrase you are optimising your page for, and this is good for not only search engines but also for the users on your site. This text will also show when there are issues with the image rendering on the site and for screen readers for users who are visually impaired – so it’s essential to have it in place. The alt tag appears in the HTML on your website as part of the image information:

4. Embed the image in a relevant web page

The context of the image within an appropriate page is another strong SEO signal. Place keyword-rich text immediately before and after the image, putting the image into context on the page. Indeed, the entire page should be optimised for the phrase the image is targeting.

5. Create internal and external links to the image

Links to images tell the search engines about the content and its relative importance. Descriptive and relevant anchor text for your links is useful and provides a better user experience.

It is useful to include keyword-rich anchor links from within your own website as well as links from external sites.
6. Include image attributes in your sitemap
You can provide additional information for Google and the other search engines in your sitemap. You can learn about image attributes in sitemaps on Google’s support site at [http://bit.ly/2OMCupw](http://bit.ly/2OMCupw).

7. Image optimising for improved site speed
When adding images to your website you need to be aware that the size of your image affects the loading speed of your website. Large, high quality images may look great but they can reduce load time of your site significantly. The key is to keep the file size as small as you can whilst maintaining good image quality. There are some useful tools that can do this for you, such as [compressjpeg.com](http://compressjpeg.com).


8. Add structured data to your images
Google uses structured data to understand the content on a page. You are able to add valuable visual indexing to your structured data for images of products (see [http://bit.ly/2OH7k2P](http://bit.ly/2OH7k2P)). Pictures clearly showing the product (for example, against a white background) are preferred. This property is required for Google Images and recommended for Google Search.


9. How to optimise your images in your CMS
When uploading an image in your content management system, eg WordPress, there are a number of fields that you need to complete in order to optimise your image thoroughly.

- **Image Title.** The title is the name of the image file and features in the optional HTML title attribute.
- **Image Caption.** To improve the user experience a caption can help the user understand your image better and will sit underneath your image.
- **Image Alt text.** As discussed previously, the phrase that you insert here tells Google what your image is about and can improve your rankings.
- **Image Description.** Often webmasters ignore this field which allows you to write a longer description of your image and is shown in the attachment page for your image.

10. Image licensing
Image licensing is important to consider if you are not using your own images. See our article on how to find free images, which points to 40 different sources, at [http://bit.ly/35vCkcV](http://bit.ly/35vCkcV).

11. Images and social media
Images are a great way to boost social shares on your website. Adding social share buttons to your website means that your images can easily be shared across the web.

Right to be forgotten on Google applies only in EU

Much has been written about the problems surrounding permanence of data once it has been uploaded to the internet - whether it's a misjudged Twitter comment by a politician from 10 years ago, or a risqué photo from bacchanalian university days which emerges when someone is looking for a job. The difficulty of erasure impinges on a broader philosophical principle - the right to be forgotten - but this term has been most commonly used to describe the stickiness of search results within Google. The specific legal question often asked in this regard is: does Google need to delete search results upon request by individuals?

Back in 2014, a legal principle was established by Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (aka “Google Spain”) whose effect was to force Google (and other search engines) to purge (or, more accurately, de-reference) search results containing personal data in respect of specific requests, as long as the information in question was “inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing.” In coming to this landmark decision, the ECJ essentially created what became known as a right to be forgotten (although in fact it was merely interpreting Directive 95/46/EC).

But the global nature of the internet presented a dilemma in respect of the legal principle established by Google Spain: should search result removal be applied on a country by country basis, for the whole of the EU or across the whole world? This question is complicated by the fact that geographical versions of Google search engines can be accessed from different locations (eg Google.fr can be accessed from the UK).

In grappling with these questions, the French privacy regulator (CNIL) argued that Google should de-reference search results globally and imposed a fine, resulting in an ECJ clarification of this point in [Google vs Commission nationale de l'informatique et des libertés (CNIL)](http://bit.ly/2O7z1pZ) in September 2019. The ECJ ruled that search results only need to be removed in respect of geographical versions of the Google pertaining to Member States – not globally. However, it also decided that Google should “put in place measures discouraging internet users from gaining access, from one of the Member States, to the links in question which appear on versions of that search engine outside the EU”.

Although this ruling appears to clarify the position on the right to be forgotten, it should be noted that a separate ECJ ruling, [Glawischning-Piesczek v Facebook](http://bit.ly/2OMCupw), held that Member States could order internet platforms to remove illegal content worldwide. This related to a complaint by politician Eva Glawischning-Piesczek to Facebook requesting the removal of comments. Commenting, Thomas Hughes, executive director of human rights organisation Article 19, noted “The ruling also means that a court in one EU member state will be able to order the removal of social media posts in other countries, even if they are not considered unlawful there.” - Alex Heshmaty.
Getting to know deepfakes

By Kelsey Farish

Deepfakes are a form of digital impersonation, in which the face and voice of a person can be superimposed into video and audio recordings of another individual. Much has happened from technological, social and legal perspectives since deepfakes first surfaced in 2017.

Deepfakes are now mainstream

2019 has seen deepfakes go from niche novelty to mainstream phenomenon. As any moviegoer knows, computer-generated special effects are nothing new. But deepfakes have captured the public’s imagination because they can be created with startling accuracy using only a few “source” images.

Deepfakes were first used in 2017 as a tool to digitally superimpose the faces of famous actresses into pornographic videos. Over the last two years however, the deepfake trend has spread beyond the world of celebrities and adult entertainment. Recent research from Dutch technology company DeepTrace (deeptrace labs.com) reports that by the end of 2018 there were just under 8,000 deepfake videos available online. As of September 2019, that number has nearly doubled to more than 14,600.

Deepfakes are often used for comedic purposes, and many purport to show actors or other celebrities appearing in funny scenarios: Nicholas Cage and Tom Cruise have made frequent appearances in a wide range of absurd film clips. By September 2019 the most downloaded mobile app in China’s iOS store was ZAO, which allows users to swap their faces with film or TV characters using just one selfie as the source image.

Creation has become easier

The deepfake creation process has become easier. Deepfakes are created by using neural networks known as deep learning, which is a subset of artificial intelligence. The earliest users of the technology were computer scientists and researchers, who developed the methods in 2012. Five years later, the codes used to generate deepfakes began to appear on public repositories and platforms, including GitHub and Reddit.

Today, only limited technical know-how is required to create a deepfake, which can be done through a variety of methods. In addition to mobile apps like ZAO, mentioned above, deepfakes can be made through graphical user interfaces or through service portals whereby users upload photos to an online platform. For those wishing to outsource the process entirely, creators can be hired through gig economy marketplaces such as Fiverr. Furthermore, hundreds of YouTube and blog post tutorials are available to help novices develop their skills.

The risks are becoming clearer

People have started to understand the risks that deepfakes pose. By way of recent example, in May 2019 a doctored video of American congresswoman Nancy Pelosi went viral on social media. The video appeared to show Rep Pelosi slurring her words in a drunken manner and was covered widely by news media. Although not strictly a “deepfake” because the methods used to distort the video were more rudimentary, this was an example of audiovisual manipulation which, together with other similar deepfakes of politicians, attracted wide media attention. Accordingly, it is now widely acknowledged and understood that deepfakes can be used for nefarious purposes. These include the manipulation of civil discourse, interference with elections and national security, fraudulent submissions of documentary evidence, as well as the erosion of trust in journalism and public institutions.

Deepfakes can also be used to harm individuals as tools to intimidate, extort, humiliate or defame. Many deepfake creation communities and forums are located on deepfake pornography websites as well as forums including Reddit, 4chan, 8chan, and Voat. It is worth noting in this instance that 4chan and 8chan have infamous reputations for hosting extremist content or even promoting illegal activity. By way of recent example, an energy executive was conned into handing over £200,000 to fraudsters who used a deepfaked voice recording of his boss.

As mentioned above, this is particularly concerning for non-celebrities too, because the social media profile that the average person establishes online provides easy access to photographs and videos, all of which may be used as source material for a deepfake.

Legislators are responding

New, specific laws have been proposed and passed to address deepfakes. There are indeed many existing laws which can potentially be applied to problematic deepfakes, including those concerning fraud, privacy, defamation, stalking and electoral law. But are these legal instruments sufficient to address deepfake risks or are new laws needed? Given the risk that deepfakes pose, some lawmakers assert that new, specific regulations are needed to curtail the proliferation of the technology. There are two broad categories of law which can be used to potentially prevent or mitigate the unwanted proliferation of deepfakes. These are sexual harassment and privacy laws on the one hand and disinformation and electoral laws on the other.

Sexual harassment and privacy laws

Legislatures in the United States as well as the United Kingdom have for several years now sought to address online sexual harassment, with numerous jurisdictions criminalising so-called “revenge porn”. In July 2019, the US state of Virginia enacted House Bill No 2678, becoming the first law to address the dissemination or sale of “falsely created videographic or still images”. The law updates the existing revenge porn laws, making it a misdemeanour to share deepfake photos or videos of a sexual nature without the consent of the subject. Similarly, the state of New York has proposed an amendment to existing civil privacy laws. A08155, which is currently pending in the State Senate, would include “digital replicas” as protectable assets of...
an individual’s persona (or personality, as known in Europe).

In the United Kingdom, the Law Commission is now conducting a review of the existing criminal law with respect to taking, making and sharing intimate images without consent. This specifically includes potential revisions to the revenge pornography provisions under section 33 of the Criminal Justice and Courts Act 2015, voyeurism offences under section 67 of the Sexual Offences Act 2003, the Voyeurism (Offences) Act 2019, exposure under section 66 of the Sexual Offences Act 2003, as well as the common law offence of outraging public decency.

**Media disinformation and electoral laws**

The second broad category of potential legislation concerns media disinformation and electoral law. This is of particular importance in the United States, given that Americans are about to enter peak campaigning for their 2020 Presidential election cycle.

In September 2019 Texas became the first state to pass a law regarding political deepfakes. SB751 amended existing electoral law to establish a misdemeanour for creating deepfake videos “with intent to injure a candidate or influence the result of an election” if published and distributed within 30 days of an election. California quickly followed suit in October with the passage of AB-730 which criminalises the distribution of audio or video that gives a false, damaging impression of a politician’s words or actions within 60 days of an election.

The US Congress has also proposed a federal law which is currently before various subcommittees for review. The aptly-titled Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability (“DEEPFAKES Accountability”) Act of 2019 seeks to combat the spread of disinformation through restrictions on deepfake video alteration technology. As currently drafted it would establish (amongst other things) a right on the part of victims of synthetic media to sue the creators and/or otherwise “vindicate their reputations” in court.

**The platforms are starting to take action**

In addition (or as an alternative) to legal safeguards, technology companies have started to take action to combat deepfake creation and proliferation. While it may be natural to assume that legislation could shield us from harmful deepfakes, the reality is far more complex.

Firstly, the laws mentioned above may not withstand judicial scrutiny from free speech and civil liberties perspectives. Secondly, while a problematic deepfake may be blocked in one jurisdiction, a lack of harmonisation at international level may allow it to spread easily to other parts of the world. Thirdly, and perhaps most importantly, because bad actors can easily remain anonymous online, the prospect of viable enforcement remains doubtful at best.

To fill the regulatory void 2019 has seen technology companies step in to take corrective action. Twitter, Reddit and even the world’s largest pornography website have officially banned deepfake videos from appearing on their platforms. Facebook and Microsoft have joined forces to form the Deepfake Detection Challenge, with $10 (£7.8) million for research and prizes. Likewise, Google has released a dataset of 3,000 deepfake videos in an effort to support researchers working on detection tools.

It remains to be seen if the legal or technological progress made in 2019 will be enough to mitigate the risks associated with deepfakes. Until then, public awareness and internet literacy may be the most useful tools.

Kelsey Farish is a technology and intellectual property solicitor at DAC Beachcroft LLP in London.

Email kfarish@dacbeachcroft.com, Twitter @KelseyFarish.

Image Detecting deepfakes, cc by-nd Siwei Lyu.
What is data misuse?

By Alex Heshmaty

Data misuse is often discussed alongside cybersecurity, within the overall context of data protection; but it is important to make the distinction between data which has been obtained legitimately but misused and data which has been collected illegally (eg without consent) or stolen (via computer hacking).

Data theft generally involves a cyber attack or harvesting of data by other means where data subjects are unaware of the collection or modification of their data; this type of cybercrime is largely covered by the Computer Misuse Act. Even where the data is provided knowingly and willingly, its collection may still be illegal if it breaches the Data Protection Act (DPA) or General Data Protection Regulation (GDPR).

The term “data misuse” is normally applied to personal data which has been initially willingly and legitimately provided by customers to a company, but is later used (either by the company or a third party) for purposes which are outside the scope of legitimate reasons for the initial data collection. This is what we will be discussing in this article.

Examples of data misuse

There have been many well publicised examples of data misuse, from Big Tech through to Brexit:

- Twitter recently admitted that it “inadvertently” used the personal information of its users, which it collected on the pretext of security purposes, to enhance targeting of advertisements.
- Google is the subject of an investigation by the Irish data regulator, which has accused the search engine of “exploiting personal data without sufficient control or concern over data protection.”
- Jeff Bezos does not escape scrutiny either, with Amazon subject to an investigation by the EU competition watchdog, preliminary findings of which claim that the company “appears to use competitively sensitive information – about marketplace sellers, their products and transactions on the marketplace.”
- The Leave.EU pro-Brexit group, which was co-founded by businessman Aaron Banks, and his insurance business Eldon Insurance, have both been fined by the Information Commissioner’s Office (ICO) for using personal data interchangeably.
- Information Commissioner Elizabeth Denham said, “It is deeply concerning that sensitive personal data gathered for political purposes was later used for insurance purposes; and vice versa. It should never have happened.”
- The ICO is investigating the AdTech industry more broadly, in particular looking at “how personal data is used in real time bidding (RTB) in programmatic advertising” and has raised concerns about how data is shared: “the scale of the creation and sharing of personal data profiles in RTB appears disproportionate, intrusive and unfair, particularly when in many cases data subjects are unaware that this processing is taking place”.
- Facebook has continued to face allegations of data privacy failures in connection which the sharing of user data with other tech firms, following on from the Cambridge Analytica scandal.

How is data misuse being tackled?

Until recently, the debate around data protection has tended to focus on cybersecurity; how to prevent personal information being stolen by “the bad guys” and put to use for malevolent ends (eg hacking into someone’s bank account). But just as computer hacking is not all black and white (there are also “grey hat” hackers!) it has become apparent that companies which legitimately collect personal data do not always use this data ethically.

In response to these grey areas – and in an attempt to redress the power imbalance between individuals and large corporations – laws are gradually being implemented by governments around the world to try and protect their citizens from having their personal data misused for profit.

The European Union is notably progressive in tackling data protection concerns. In 2018 it implemented the GDPR which contains a range of measures designed to protect personal data, of which the principle of purpose limitation is particularly directed at data misuse – article 5(1)(b) states that “Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”

But it is not just Brussels regulating to empower individuals with rights over their personal data; California has introduced its own scaled down version of the GDPR – the California Consumer Privacy Act (CCPA) – which comes into force at the start of 2020 and, amongst other measures, allows individuals to opt out of having their personal information sold on to third parties.

Although regulation is vital in tackling data misuse, Big Tech is also taking its own steps to self-regulate, a good example of which is Google’s Developer Data Protection Reward Program which pays out “bounties” to developers who “identify situations where user data is being used or sold unexpectedly, or repurposed in an illegitimate way without user consent.”

What does the future hold?

The current primary challenge in relation to data misuse is arguably about reaching a consensus.
regarding the rights of data subjects to maintain control over the use of their data which is held by companies, governments and other organisations. In a recent lecture on “Algorithms, Artificial Intelligence and the Law” Lord Sales touched on the importance of democracy and national government in tackling a whole array of issues facing a digital world, including data misuse:

“In elections, the detailed information about individuals harvested by computing platforms allows voters to be targeted by messaging directed to their own particular predilections and prejudices, without the need to square the circle of appealing to other points of view at the same time. We need to find ways of reconstituting a common public space.”

Ultimately, more legislation is necessary to define and regulate data misuse. Perhaps the most difficult piece of the puzzle lies in achieving multi-jurisdictional agreement, where liberal governments wrangle with more authoritarian regimes, also highlighted by Lord Sales when he alluded to “China’s social credit system, in which computers monitor the social behaviour of citizens in minute detail and rewards or withholds benefits according to how they are marked by the state.”

But whilst legislators decide how to reach the right balance between allowing free data flows to help commerce and protecting the rights of citizens to control their personal information, digital innovation continues to forge on with new products and services – many of which revolve around collecting increasingly personal data (eg with the rise of MedTech).

Further reading


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). Email alex@legalwords.co.uk. Twitter @alexheshmaty. Image cc by Book Catalog on Flickr.

California passes landmark gig economy rights bill

The rise of the gig economy and zero hours contracts – often facilitated by the internet and apps such as Uber, Deliveroo and Limber – has been the subject of vigorous debate over recent years. Governments across the world have been grappling with the implications for employment law and wider society, balancing the boost to the economy and reduction in unemployment with restrictive practices, insecurity of work, low wages and imbalance of power.

In the UK, the Government commissioned an independent review of modern working practices by Matthew Taylor (the Taylor review) back in 2017. One of its primary aims was to consider the challenges of the gig economy model and provide recommendations to tackle any problems. Although the Government went on to introduce new legislation on the back of the Taylor review in late 2018, it was criticised as failing to make any real impact on the gig economy or zero hours contracts. In particular, the fact that most individuals working in the gig economy continue to be classed as “self-employed” means that fewer people are able to take advantage of employee rights.

In California – where many of the apps which provided the engine for the gig economy originated, and where there are an estimated 1 million gig economy workers – legislators seem to be making some significant progress in an attempt to rebalance power. Assembly Bill 5 aims to implement a new law which would lead to more gig economy workers being classed as employees and consequently able to claim holiday and sickness pay.

Uber in the UK is currently appealing to the Supreme Court in respect of previous court decisions that its drivers should be treated as “workers” – and it is separately facing licensing problems in London. Most recently, Transport for London (TfL) has said it will not grant it a new licence due to alleged safety failures. TfL says “it is unacceptable that Uber has allowed passengers to get into minicabs with drivers who are potentially unlicensed and uninsured.” Uber can continue to operate in London while it appeals the decision. – Alex Heshmaty
**Who owns an AI-generated invention?**

By Katharine Stephens

One wet Sunday afternoon I was playing with an interface to OpenAI’s machine learning model, GPT-2, which was trained to predict the next word in a sentence and which can now generate articles of synthetic text based on a sentence provided to it. I typed, “Can AI own the copyright in the work that it has generated?” After a little pause, I would like to say for thought, the AI provided some text which did not make redundant the writing of this article but nevertheless was grammatically correct and very readable. It ended with a flourish saying, “and that is a philosophical, not a legal, question.”

Amusing, but increasingly and sometimes disconcertingly “human”, AI is now part of our daily lives. It finishes our sentences (for example, Gmail’s SmartCompose), it finds the information we need on a myriad of topics (think of Alexa and other voice assistants) and it curates the ads and news we view online [Note 1]. It is also doing things which we think of as being the exclusive reserve of humans; it is creating art works and writing music.

Not only that, but it is also very “clever”. DeepMind’s neural network, AlphaGo Zero, taught itself the complex game of Go and after three days beat its predecessor, AlphaGo, which had itself beaten the 18-times world champion. Other AI models are helping scientists discover new drugs and develop innovations in clean energy.

This raises interesting questions for intellectual property (“IP”). When AI writes an article, paints a picture or creates some music, who owns the resulting copyright in the work? When AI develops a new idea which might be patentable, who owns the invention?

### Who owns an AI-created work?

In order to answer this question, you have to ask first: who is the author of the work? The author is the person who creates the work and will be the first owner, unless that person is an employee in which case the copyright is owned by their employer. As is apparent from this summary of the law, creating a work is essentially a human activity. This is supported, if support is needed, by reference to the automatic transfer of copyright from employee to employer; AI cannot be said to be an employee.

But how do AI created works fit into this scheme? At one end of the scale where someone has used a computerised tool, such as text editing software, to help them compose an article, that person will still be the author of the literary work if the work is original. To be original, a work must be an author’s or artist’s own intellectual creation, reflecting their personality (see the decisions of the EU Court of Justice in Infopaq, C-5/08, and Painer, C-145/10).

At the other end of the scale, a human who simply provides training data to an AI system and presses “go” is unlikely to be considered the author of the resulting work. An example might be “The Next Rembrandt” a unique 3D-printed painting created by an AI system which mimicked Rembrandt’s style, including his brushstroke technique. Those who worked on this fascinating project have pointed out that the AI produced the painting solely from being trained on a dataset of Rembrandt’s paintings.

In most countries, if no human author can be identified for the work, no copyright will subsist in it and therefore it will fall into the public domain. Although there may be copyright in the AI algorithm itself, as computer programs are protected by copyright, this is a separate work whose authorship (and ownership) is separate from the work it creates.

However, in the UK, the law makers have been ahead of the game. Wanting to encourage investment in AI in the 1980s, Parliament created a category of “computer-generated works” in section 9(3) of the Copyright Designs and Patents Act 1988 (CDPA). These are works which are generated by a computer in circumstances where there is no human author. The author is therefore deemed to be the person “by whom the arrangements necessary for the creation of the work are undertaken.” To date, there has been no case law to answer the question of whether there is any requirement of originality for computer-generated works under section 9(3) [Note 2]. Some commentators say there is no such requirement. Some say that there is, but then disagree as to where it should lie, being split as to whether there should be originality in making the arrangements to generate the work or whether the work itself should be original when judged objectively.

Another issue that may well arise in the future is one of joint ownership. If there is a scale with human generated works at one end and computer generated works at the other, there will be an area between them where it could be said that the human and the AI jointly contributed to the work. Joint ownership is a difficult enough question to answer between human authors [Note 3] and can be a very hard fought issue since one co-owner can prevent another co-owner from exploiting the work without their permission.

### Who owns an AI-generated invention?

The inventor is the first owner of any patent which is applied for and granted over that invention. As the law currently stands, AI cannot be the inventor (and therefore the owner of a patent) because “devising” an invention is a human activity which involves contributing to the inventive concept. The invention and any patent granted over it will, as a consequence, belong either to the human deviser or, if an employee, their employer.

As noted above in relation to copyright law, there is a scale with, at one end, AI being used as a tool, admittedly a very sophisticated tool, to help develop new inventions. Where AI has been part of the inventive process in this way, it is arguably no different to using any other tool, such as a microscope. The inventor will therefore be the person using the AI. Mere ownership of the AI system would not qualify someone to be an inventor.

At the other end of the scale where AI is devising the invention with no human intervention, then, under the current law, no one can claim to be the inventor and it will not be possible to protect the invention by
applying for a patent, although this has not stopped a few people from trying. For example, the University of Surrey has announced that its creation machine, DABUS, is named as the inventor of a new food container and patent applications in its name have been made in the UK, the USA and at the European Patent Office. Possibly in response, the UK Intellectual Property Office (IPO) has, in its most recent update to its Formalities Manual, added a statement that “An AI Inventor is not acceptable as this does not identify ‘a person’ which is required by law. The consequence for failing to supply this information is that the application is taken to be withdrawn.”

What of the future?

Is the IPO’s response the correct one for the long term? It could be argued that it could lead to the arbitrary naming of an “inventor”, whether they have devised the invention or not, in order to prevent the invention from falling into the public domain.

Although at first glance, this might look as if it benefits society, will that actually be the case?

If the system were to be changed and AI considered to be an inventor, rules would then have to be laid down as to who should own the resulting patent. Questions would then need to be asked as to who or what society wants to reward? Should it be the owners of an AI system? Should investment alone ensure a stake in the resulting work? Changing patents into pure economic rights would be a very significant change to the system and significantly affect the industries which rely upon such assets.

In relation to works protected by copyright, AI is getting so good at creating art and music that it is increasingly difficult to tell what has been generated by AI and what has been generated by a person. If an AI-generated work is free to use because no copyright protects it, what will happen to works generated by human authors? Will humans be able to compete in the marketplace with AI-generated material?

One solution could be to award “personhood” to AI, but I believe that it is far too radical a step to take. Another solution is to have a deeming provision for all IP rights generated by AI similar to that found in section 9(3) CDPA, which at present has only been adopted by the UK and one or two other countries.

These questions and more, challenging the settled notion of IP ownership, are currently the subject of much debate [Note 4]. Perhaps OpenAI’s text generator was correct: if AI is going to change our view of what it means to create and own a work of art, that is a philosophical rather than a legal question. But it is one that IP professionals and governments are going to have to tackle.

Notes and further reading

1. For a discussion of personalised news and the impact on editorial values, see “Using artificial intelligence in news intelligently: towards responsible algorithmic journalism” posted on LSE’s Media@LSE blog at http://bit.ly/2XJ80Jc.

2. One of the few cases relating to section 9(3) CDPA is Nova Productions v Mazooma Games [2007] EWCA Civ 219, where it was held that a person playing a computer game was not the author of screenshots taken while playing the game and had not undertaken any of the arrangements necessary for the creation of the images. Instead the court held that the persons who made the arrangements necessary for creation of the screenshots were the game’s developers.

3. The Court of Appeal has recently ordered a retrial in Kogan v Martin [2019] EWCA Civ 1645 on the question of whether there is joint ownership in the screenplay of the film “Florence Foster Jenkins” about the eponymous American socialite who believed herself to be a talented operatic singer.


Katharine Stephens is a partner and the co-head of the London intellectual property department of the law firm Bird & Bird LLP.

Email Katharine.Stephens@twobirds.com.

Twitter @twobirdstech.

Access to justice through technology: the providers

By Nick Holmes

The Law Society, in its report Technology, Access to Justice and the Rule of Law, published September 2019 (http://bit.ly/lawsocA2J), defines the “Access to Justice Sector” as “Comprised of all organisations supplying access to justice services. It includes law firms, Not for Profits, individual practitioner barristers and solicitors, in-house legal teams, government bodies, academics, LawTech businesses and associations.” This is not very helpful, but nevertheless true. Everyone involved in the legal sector is involved in delivering (access to) justice in some way, though we might debate the merits.

The third sector

In the field of frontline services providing education, information and advice, the third sector leads, often working with firms and universities. The Law Society report provides many examples of such services, with an exemplar service cited for each type of innovation overcoming a particular barrier to access to justice. Curiously, whilst the report contains a bibliography, it does not also provide URLs for the exemplar services it cites. When asked about this, a Law Society representative gave this baffling reply:

“I am afraid we are unable to share this data. A number of participants of our study requested that their initiative was kept confidential, therefore this information was purposely left out of the report.”

I’ve remedied that with the list below.

The Society’s research revealed a significant problem, with the market of A2J providers not wanting to share resources. Apart from the inevitable entreaty for the Government to commit to providing necessary funding, most of their recommendations relate to the Government and private and third sector organisations sharing or open sourcing information and co-ordinating and collaborating on plans to prevent duplication.
Solicitors practices

In addition to the pro bono efforts from both sides of the profession, solicitors practices are at the sharp end of facilitating access to justice by providing affordable legal services.


“The current set of recommendations leans heavily on suggestions for government action. These are worthy; can be called in aid to defend the Society; but are likely to be of little direct help to members. ... What could the Society produce on technology that would be read with interest and benefit by, for example, a two person firm in Newcastle; a sole practitioner in Birmingham and a group of young solicitors thinking of establishing a practice in Walthamstow? They currently feel bewildered by change; battered by cuts; distrustful of the Society; and uncertain of the way forward. What can we give them to help?”

He has a number of recommendations for the Society, but ultimately, “how can a practice successfully deliver high quality legal services to low income clients?”

Government

HMCTS’s Court Reform Programme, established in 2016, aims to introduce new technology and working practices to make the justice system more accessible (http://bit.ly/HMCTSreform). This is a £1bn programme involving over 50 projects across the civil, criminal and family courts and has achieved much already. However, a Commons Select Committee reports that it is still struggling to deliver all it promised and has not shown it is doing enough to understand the impact on court and tribunal users before pressing ahead with reforms (http://bit.ly/HMCTSreform2a).

“To date its evaluation has largely been process-based, focussing on how new technology is working rather than the impact on people or justice outcomes. ... Although some digitised services like divorce seem to be working well, [some] are concerned about how online services may disadvantage users with low digital or legal literacy.”

Responding to these criticisms, HMCTS CEO Susan Ackland Hood says that “more than 250,000 members of the public have used our new online services since last year with over 80 per cent satisfied. Many of those users have told us that such services ... have given them access to justice not previously available.” A fuller response will follow (http://bit.ly/HMCTSreform3).

Other online providers

There are many other online providers operating in the DIY law space. Undoubtedly they contribute to access to justice, but we'll address them another time.

Third sector A2J exemplar services

This list is derived from section 5 of the Law Society’s report (discussed above), with added links.

Back-office services

1. Case and legal process management.
   Citizens Advice: Casebook
2. Means testing to enfranchise vulnerable persons.
   Legal Education Foundation & Law Centres Network
   CourtNav
   Law For Life
3. Empower advisers and internal stakeholders through education.
   Frontline Immigration Advice Project

Front-office services

1. Public legal education tool to help people identify the nature of the problem and when there is a need to consult a solicitor.
   The Mencap ChatBot
2. Accessible information to enable people to assess their entitlement to benefits or eligibility for legal aid.
   Legal Aid Eligibility Calculators
3. Customised legal information and education which is easy to access and understand.
   Legal Utopia
4. Alternative dispute resolution processes.
   Yess Law
5. Support for legal document assembly.
   Personal Independence Payment Tools
6. Introducing users to organisations that can provide information, advice and advocacy.
   [Explanation of Guided Pathways – no examples cited.]

Nick Holmes is Editor of this Newsletter.
Email nickholmes@infolaw.co.uk. Twitter @nickholmes.

With our Internet for Lawyers CPD 2019 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. These are saved online so you can print out whenever required.

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.

Complete your 2019 CPD now at infolaw.co.uk/cpd. Only £90+VAT (group rate £50+VAT)