Internet law pre- and post-Brexit

By Graham Smith

To launch a new edition of a legal textbook in the very month that the UK is about to leave the EU – let alone a book focused on the internet at the height of the techlash – may seem a little reckless.

Or perhaps not. Internet law stays still for hardly a moment anyway. The couple of months since the 5th edition of Internet Law and Regulation went to press have already seen two domestic High Court decisions, one CJEU judgment and an Advocate General Opinion all on copyright communication to the public; not to mention three CJEU Advocate General Opinions on government powers to mandate communications data retention for law enforcement and security. As I write, regulations have been laid to implement the UK-US Agreement facilitating cross border data and interception requests direct to online service providers. A textbook in this field is inevitably a snapshot of a rapidly changing landscape.

Divergence from EU law

The new edition’s snapshot is taken at the moment when the UK starts to think about forking away from the influence of EU law. How far and fast it will do so after the transition period expires is still largely an imponderable. The UK’s room for manoeuvre will depend on the outcome of the coming negotiations for a trade agreement. In some areas it may be constrained by the desire to obtain a data protection adequacy decision from the European Commission.

If Brexit can be considered a project, then in business process modelling terms this edition is the “as is” analysis of internet law that precedes the post-Brexit “to be” – a reference point at a crucial juncture against which to measure divergence as time goes on.

Generally speaking, EU law will (if not already implemented as domestic UK legislation) automatically be continued as domestic UK law after the end of the transition period unless and until regulations or Parliament do something different by amendment or repeal. However, the Charter of Fundamental Rights will not continue. The extent to which courts will be able to depart from existing EU Court of Justice decisions after the end of the transition period is subject to regulations made during the transition period.

Mutual recognition

The most immediate changes after the end of the transition period will be in areas that depend on mutual recognition between EU countries, such as the internal market aspects of the ECommerce Directive. No longer will a UK defendant sued in another EU court be able to prevent application of more restrictive laws of the forum to its service provided from the UK, as happened in Martinez v MGN Ltd (C-161/10, 25 October 2011). No longer will PhonepayPlus, the premium rate phone regulator, have to invoke a derogation from the Directive in order to fine non-compliant online services provided to the UK from other EU Member States.

We will also bid farewell to the Transparency Directive, with its prior notification requirement waiting to trip up the unwary legislator who ventured into the field of information society services. The DCMS fell foul
of the Directive twice: once with the Video Recordings Act 1984, which had to be re-enacted in 2010 after the discovery that it had not been notified 25 years earlier; and more recently with un-notified guidelines under the Digital Economy Act 2017.

Mutual recognition arises in other areas. The eIDAS Regulation requires Member States to recognise qualified trust providers (which underpin qualified certificates) registered in other Member States. While the UK has already decided that it will continue to recognise providers registered in EU Member States, the converse would not be the case after the transition period unless recognition formed part of the trade deal.

Country of origin regimes such as under the Satellite and Cable Broadcasting Directive, the Audiovisual Media Services Directive and the Net Portability Directive would cease to apply to the UK. The post-transition period status of existing UK holders of .eu domain names remains uncertain.

**Maintaining the ECommerce Directive**

There is likely to be close focus on the intermediary liability shields derived from the ECommerce Directive. Even assuming that the government maintains the principle of alignment with the Directive as its policy, the mechanics of keeping legislation aligned present a formidable administrative challenge.

That is because the 2002 ECommerce Directive Regulations, which initially implemented the non-financial services aspects of the Directive, did not have prospective effect.

Since 2002, therefore, each time a new piece of legislation has been enacted that might impose liability on a conduit, cache or host, the government has had to remember to include the required liability shields in the legislation. The same has applied when any pre-2002 legislation was amended or re-enacted. Sometimes, inevitably, the government forgot to do it. But the gap could relatively easily be filled by passing secondary legislation under the European Communities Act 1972.

As a result we have a complex patchwork of primary and secondary legislation implementing the Directive, numbering nearly 30 separate items at the end of 2019.

Whether the government will be assiduous in including the liability shields in future legislation and how, in the absence of the ability to pass secondary legislation under the 1972 Act post-transition period, it would go about filling gaps when it forgets, are matters for conjecture.

Relatedly, Article 15 of the ECommerce Directive prohibits Member States from imposing general monitoring obligations on conduit, caching and hosting intermediaries. That operates in two ways: it bars the UK from legislating to impose such an obligation, and it requires the courts to observe the prohibition when granting injunctions and applying common law rules. The second aspect probably counts as retained EU law and would continue after the end of the transition period. The first, however, would fall away: Parliament could in the future enact legislation that imposed a general monitoring obligation.

**Surveillance and data retention**

Since the 4th edition of the book appeared in 2007, surveillance of communications by law enforcement and intelligence agencies has come to the forefront – in part due to the Snowden revelations in 2013. Lord Anderson QC’s 2015 report “A Question of Trust” described the Regulation of Investigatory Powers Act 2000 (RIPA) as incomprehensible to all but a tiny band of initiates. Although the 4th edition dwelt to a degree on RIPA, the legislation unfolded its inner secrets only as litigation brought by various NGOs proceeded through the Investigatory Powers Tribunal.

Now we have the Investigatory Powers Act 2016, which has codified the full range of targeted and bulk investigatory powers ranging from interception to equipment interference, and which introduced independent prior approval of most powers. A complex web of litigation over surveillance and communications data retention powers is proceeding in the UK domestic courts, the CJEU and Strasbourg. Whilst the direct influence of CJEU decisions may wane after the end of the transition period, they will continue to have indirect influence over negotiations for a data protection adequacy decision. As the USA has discovered with its Safe Harbour and, now, Privacy Shield the CJEU may exert its influence from afar where cross border transfers of personal data are concerned.

**Copyright and intermediaries**

The potential ability to diverge post-Brexit may provide opportunities to address anomalies such as the personal copying for private purposes copyright exception, which would have legalised the universal practice of ripping CDs to personal digital devices. It was struck down on the grounds that the government had not properly considered whether the exception was de minimis for the purposes of the EU InfoSoc Copyright Directive. After the close of the transition period the government would be free to re-implement the exception, should it wish to do so.

The EU Digital Copyright Directive adopted in April last year has to be implemented in Member States by 7 June 2021. Assuming no extension to the transition period, the UK would not be bound to implement it. Indeed the government revealed in answer to a Parliamentary Question on 21 January that it does not intend to do so, and that any changes to the UK copyright framework will be considered as part of the
usual domestic policy process.

The EU is also embarking on proposals for a Digital Services Act at the same time as the UK government is considering legislation following its Online Harms White Paper.

The next few years will not be short of activity in the internet law field. In an ideal world would we start from here? Probably not. But if this new edition of the book helps the reader understand what “here” looks like, it will have achieved some of its purpose.

Graham Smith is Of Counsel at Bird & Bird (twobirds.com) specialising in internet, IT and intellectual property law. He is the author of Sweet & Maxwell’s *Internet Law and Regulation* and blogs as Cyberleagle (cyberleagle.com).

Email Graham.Smith@twobirds.com.
Twitter @cyberleagle.
Image: Public Domain CC0.

Internet Law and Regulation 5th edition

The leading title in its field, by Graham Smith and colleagues at Bird and Bird, *Internet Law and Regulation* presents an analysis of key areas of internet law and regulation. The 5th edition is fully updated to include recent developments relating to GDPR, the Investigatory Powers Act 2016, eIDAS, online intermediary liability, including site blocking injunctions and updated UK and EU case law.


Public Information Online

By Paul Magrath

Public Information Online (PIO) www.publicinformationonline.com is an online database provided by Dandy Booksellers, who are well established suppliers of official government print publications. The PIO database collects and provides access to digitised parliamentary papers going back for more than a century.

The material held includes Public General Acts since 1900, House of Lords Papers from 1901, Hansard debates from 1909, House of Commons Bills from 1919, Public Bill and General Committee Debates from 1919, House of Commons Papers from 2006/07, together with more recent collections from the devolved Scottish Parliament, Northern Ireland Assembly and National Assembly for Wales, as well as Command Papers going back to 1955 and non-parliamentary papers such as Law Commission papers, Audit Commission reports and so on. Although some of this material is available in the public domain elsewhere, eg on Parliament’s own website from the start of the 21st century, or via The National Archives, the fact that it can be searched together in one place is a great benefit.

Pepper v Hart

As well as offering general access via search and browse to all this material, PIO also offers its dedicated Pepper v Hart service to assist researchers wishing to cite parliamentary material as an aid to statutory construction in court. Essentially, what Pepper v Hart [1993] AC 593 permits is:

“reference to Parliamentary materials where (a) legislation is ambiguous or obscure, or leads to an absurdity; (b) the material relied upon consists of one or more statements by a minister or other promoter of the Bill together if necessary with such other Parliamentary material as is necessary to understand such statements and their effect; (c) the statements relied upon are clear.” (Per Lord Browne-Wilkinson at p 640.)

The Pepper v Hart service harnesses all the parliamentary material on PIO in order to provide, for any particular Bill, a list of all the documents or debates in which it is discussed. It works like this. You select the collection, which will usually be the UK Parliament. Then you select the session, which should be the one in which the relevant bill was passed. Having selected the session, you are given an alphabetical list of Bills or Acts. Having chosen the relevant statute, you are then presented with a list of publications in which it is discussed. Within each publication, you can search for a relevant phrase or quotation.

At this point, you have two options. Either you can open and search within each of the listed documents. Or you can perform a search on all the documents, which will narrow down the list of results, then click on “view selected documents” to display the pages from those documents that contain the highlighted search terms identified. These pages can be removed if not relevant, or added to by adding at any point the next or preceding page. You then have a PDF document, which you can download, containing all the relevant passages to your query. This avoids the need to print out the whole of any document, if all you want is a page or two extracted from it.

There is of course nothing to stop you downloading an entire document and using that for more detailed research. But the advantage of the way the online search works is its convenience, particularly if you are looking for a particular expression in the statute whose meaning is ambiguous or unclear.

While it takes a bit of practice, and works better for some queries than others, there seems to be nothing comparable to this service on any other legal information platform. It cannot be faulted for convenience and ease of use, and I understand that the search functionality is being further developed. (I look forward to being able to use Boolean connectors to conduct more targeted searches, for example.) Even as it stands, I would certainly recommend it as a lot easier and more convenient than the traditional method of scanning all the relevant printed materials by hand.

Paul Magrath is Head of Product Development and Online Content at the Incorporated Council of Law Reporting (iclr.co.uk).

Email paul.magrath@iclr.co.uk. Twitter @maggotlaw.
Establishing trust online

By Alex Heshmaty

"I read it on the internet" has become a phrase which often generates mockery and epitomises gullibility or naivety about the online world. In the 1950s science fiction writer Theodore Sturgeon proclaimed that “ninety percent of everything is crud” which came to be known as Sturgeon’s Law. One can only speculate as to how Sturgeon may have adapted the percentage value of his law had he lived in the age of cat memes and online trolls.

Although awareness of the phenomenon of “fake news” has only gathered momentum since Trump started issuing proclamations on the veracity of mainstream media, separating the wheat from the chaff of online content has been a challenge ever since Joe Bloggs was given the power to blog. Social media has not only amplified the reach of anyone who wants to express their own version of the truth – without the editorial constraints of journalism (such as basic fact checking) – but it has also provided a commercial incentive, apropos surveillance capitalism, to create yet more content to be consumed by a willing audience.

Paul Bernal argued in the January 2019 issue of this Newsletter that the very eco-system of much of today’s internet, fuelled by the collection of personal data, which generates such huge profits for Silicon Valley – and its reliance on content creation by third parties to gain an audience and subsequent advertising revenue – indirectly encourages false information to be propagated online and perpetuates the fake news cycle. Ironically, the very structure upon which their businesses are based is causing headaches for the major internet platforms, along with their biggest clients. For example, a recent study by activist group Avaaz found that over 100 top brands had adverts running alongside YouTube videos which were actively promoting false information about climate change.

Although many of the social media companies claim to be taking steps to combat the proliferation of fake news, as part of overall efforts to moderate content, they still have a long way to go. Facebook announced plans to clamp down on political misinformation ahead of the UK’s 2019 general election, but these were criticised as being profoundly inadequate, due both to a paucity number of fact checkers and because, under Facebook’s own rules, adverts from politicians or political parties are not eligible for fact checking. And although Twitter banned political advertising altogether, CEO Jack Dorsey was unable to prevent the Conservatives from rebranding one of their accounts to give the impression that it was a fact checking service!

Independent fact checking sites have sprung up in an effort to fill the truth void. Snopes describes itself as “the oldest and largest fact-checking site online, widely regarded by journalists, folklorists, and readers as an invaluable research companion.”

However, it’s not just fake news and false information which tarnishes trust on the internet. Trust in the governance of the very foundations of the internet is at threat. Until now, the .org top level domain, which denotes websites of non-profit making organisations, has been managed, in turn, by a non-profit American organisation called the Internet Society (ISOC) via its subsidiary, Public Interest Registry (PIR). But in November 2019 ISOC announced that it was selling PIR to private equity firm Ethos Capital, to the consternation of NGOs and internet activists who are concerned about growing monetisation of the structure of the internet, with consequent damage to principles such as net neutrality.

How to establish trust online

It could be argued that establishing trust is just as difficult offline as it is online. Fraudsters and charlatans have always existed, so a healthy dose of cynicism has always been a helpful tool in navigating everyday life. The problem is that the internet has created a huge industry geared towards psychological manipulation – whether this is just about targeted ads or, as with Cambridge Analytica, for political purposes. “Click farms” employ thousands of people around the world who create multiple anonymous social media accounts and generate fake likes on Facebook and misleading product reviews on Amazon. As libraries shut down – and the ones which still exist are dominated by computer terminals – people are now largely reliant upon the internet as a source for information. While governments and tech companies try and find ways of weeding out fake news and establishing trust online, there are a few measures individuals can take to reduce the likelihood of being fed misinformation:

Website. Where does the information appear? If you’re reading an established news website such as the BBC or Guardian, or conducting research on a government or NHS portal, then you can rest assured that the information is probably accurate and has been checked by editors etc. One of the problems is that many people searching for information now don’t even open a website – they rely on featured snippets which appear at the top of the Google results page.

Sources. Information on random websites should always be checked against original sources. Spurious claims are often made on the back of scientific studies – and it’s often worth searching for the original research paper and reading the abstract.

Cross-checking. Does a piece of political news seem biased? It’s always a good idea to look for alternative sources of the same news, especially in publications which may have a different political leaning. The same goes for any information; cross-check as much as possible to establish the real facts.

Social media. It’s a sobering thought that half of adults in the UK rely on social media as a source of news. Many people now simply glance at the headlines in their feeds and share these with others without even reading the articles – and, what’s worse, they are more inclined to share fake news than real news! Anything gleaned from social media must be checked against established sources of information.
Encryption: security v privacy and Online anonymity: the debate so far

Further reading

Internet Newsletter for Lawyers, Paul Bernal: Why privacy is the key to Facebook's fake news problem http://bit.ly/INL1901bernal


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: Public Domain CC0.

Encryption: security v privacy

By Will Richmond-Coggan

In August 2015, a British journalist and cameraman were travelling in Turkey, making a documentary for Vice News. As is often the case, they were working with a local agent, a "fixer" who was responsible for getting them access to the locations and subjects they wanted to include in their documentary. All three were arrested and, in September 2015, charged with deliberately aiding an armed organisation. The primary justification for the charge was reported to be the presence of sophisticated encryption software on the devices of the fixer, of a type alleged to be commonly used by terrorists.

A few months later, in California, the San Bernardino department of public health was holding a training event and Christmas party for around 80 staff. During the event, an employee of the department and his wife carried out a terrorist attack, killing 14 people and injuring a further 22. During a subsequent running battle with police, both of them destroyed their personal phones before finally being killed. The health department employee's work phone, an Apple iPhone 5C, was recovered intact by the FBI, who believed that the phone contained information which might assist their investigation of the incident.

The FBI asked Apple to give them access to the device, which was locked with a 4-digit PIN number, and encrypted. The phone was set to erase its contents if an incorrect PIN was entered 10 times. Apple told the FBI that their devices are so secure that even Apple itself is not able to gain access to them. The FBI then asked Apple to develop software which would enable the FBI to gain access, and when Apple refused the FBI commenced legal proceedings. These were eventually discontinued when the FBI said that they had found a third party willing and able to break into the device – which was subsequently found to have no information relevant to the incident stored on it.

Incidents like these, of which there are very many examples in the media, illustrate the tension at the heart of the debate around encryption and the central role that privacy through encryption has assumed in most of our lives. There will be those who imagine that they never use encryption, but anyone who has visited a secured website employing TLS (formerly SSL) protection has done so. Many mainstream communication channels, such as WhatsApp, are end to end encrypted. Devices, not only from Apple but also from other major manufacturers are either sold with encryption turned on by default or capable of being configured to protect any data stored or transmitted through the use of freely available ubiquitous encryption software.

Two sides of the same coin

The driver behind this dramatic upsurge in the use of encryption in the everyday lives of ordinary citizens is the desire for privacy, coupled with a growing awareness of the danger presented by engaging in the digital world (particularly online) without such protections in place. Encryption is what gives confidence to shoppers wanting to make purchases online, or the users of internet banking or government portals. But, crucially, it has other purposes which give rise to the tensions identified above. It can be used by dissidents, activists and journalists, looking to coordinate activities and gather information on the world’s most repressive regimes. And it can also be used by terrorists, cyber-criminals and other bad actors to conceal their identities or hide details of their plans from investigating authorities.

The reason for focusing on 2015 in the examples given above is that this was the year in which the UN Human Rights Council published a report of its Special Rapporteur on the protection and promotion of the freedom of opinion and expression, David Kaye. This report was focused largely on the extent to which encryption and similar technologies were essential for the protection of free opinion and speech, as well as other fundamental freedoms.

In the context of the Snowden revelations about mass state surveillance by the NSA and others, the report considered carefully the arguments for reducing that protection in the interests of state security. Its conclusion was that none of the arguments made could justify such a weakening of privacy through encryption. But the same arguments considered and dismissed in that report continue to be made today, even as the commercial and regulatory pressure on businesses to provide enhanced privacy to their users also continues to increase.
Understanding the balancing exercise

In order to make sense of the balancing exercise that is having to be negotiated, between national security and privacy interests, it is important to understand the options that are being proposed. It would be naïve to suggest that any form of encryption is impossible to crack, but when considering the need to obtain actionable intelligence, the critical factor is time. The strength of encryption is measured in bits (essentially the size of the key that needs to be entered to unlock the data). If you imagine a 4-digit combination padlock, you can readily appreciate that it would take 10,000 attempts to try every combination between 0000 and 9999, although you might find the one that works much sooner than that. The DES encryption standard which was pioneered in 1976 used 56-bit encryption and can now be broken routinely by supercomputers in very little time at all. AES encryption using 128-bit encryption is readily available commercially and it would take the most powerful computer currently known to exist longer than the current age of the universe to test all possible combinations. 256-bit AES encryption is believed to be uncrackable (subject to developments in the field of quantum computing).

Consequently, intelligence agencies are keen to identify shortcuts that allow them to unlock the encrypted data without having to resort to brute force attacks. As detailed in the UNHRC report from 2015, three main alternatives are proposed. These are: the deliberate weakening of commercially available encryption standards; the creation of so-called “back doors” which would allow approved state actors to use something like a skeleton key to unlock the encryption; or an arrangement called “key escrow”. This latter option involves the key that will unlock the data being held (perhaps by a trusted third party) in a way that means that it could also be accessed in appropriate circumstances by those same approved state actors.

There are practical difficulties with each of these approaches, which it is not necessary to go into for the purposes of this article. But each of the three, it is generally accepted, involves weakening the privacy protection that encryption affords – not only against state actors, but also against everyone else. Weakened encryption will be just as easy to crack for cyber-criminals as it would be for intelligence agencies. Identification of the back door key to a method of encryption would expose all of the communications sent using that encryption, and not just the specific message being investigated; and trusted third parties could be vulnerable to breaches just like any other organisation, but if compromised would expose all of their customers to risk.

The question then becomes, to what extent is that weakening of privacy (which – as the 2015 report argues – also means a weakening of the associated freedoms of speech and opinion) something that can be justified in the interests of national security? This is relevant, because the rights referred to are seldom absolute. Under art 17 of the International Convention on Civil and Political Rights, interference with these rights is only permissible to the extent that it is lawful and not arbitrary. The European Convention on Human Rights (art 8(2)) requires such interferences to be lawful and “necessary in a democratic society”. Where those conditions are fulfilled, therefore, it follows that it can be permissible to diminish or even remove those rights, to the extent necessary.

For a time, after 2015, it had seemed that the balance of this argument was shifting in a number of countries in favour of legislating for national security interests, at the expense of privacy. Recent developments however, have demonstrated that the debate is still very much alive. The GDPR (and associated domestic legislation across Europe) has provided a strong incentive for data controllers to implement encryption on an end to end basis across all of their personal data estates. The use of encryption assists with the requirement to impose adequate technical and organisational safeguards; and with the risk assessment necessary to determine other safeguards. It also plays a significant part in determining whether there has been a loss of control of data following a data breach, and whether the potential impact on the rights of affected data subjects is of a level that requires a report to be made to supervisory authorities.

Even more recently, on 15 January 2020, the Advocate General’s Opinions in Case C-623/17 Privacy International, Joined Cases C-511/18 La Quadrature du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others involving legislation requiring the retention by commercial entities of electronic records for state surveillance purposes underscored that the PECR does apply to such activities, notwithstanding the national security considerations. It seems that encryption will continue to represent a significant battleground between security and privacy, and that the tensions between those two competing objectives are no closer to being resolved.

Further reading


Online anonymity: the debate so far

By Joanne Frears

Since the internet was in its infancy, the rights of users to use it to express their opinions was sacrosanct. When the first laws of the internet were being forged by legislature and in the courts, internet service providers (ISPs) were the focus of these sacred rights and they avoided liability by claiming they were "mere conduits" of these views and not "publishers" of them (and the eCommerce Directive of 2000 confirmed this). This felt like the right approach; by not making the "engineering back office" of the internet liable for the content on it, the internet could flourish. It would remain free thinking and free to use, and freedom of speech would be preserved.

Since that time, we've seen revolutions and uprisings overthrow corrupt governments – and allowing people to remain anonymous has protected their views and their freedom. Masses of people have been empowered by access to world-wide information sources, education and communication. The world feels smaller and we’ve celebrated this.

But the flip side of the free speech coin is that trolling and online hate crimes from people who deliberately hide or obscure their identity has increased. The ability of a person to remain hidden on the internet draws as much criticism as the right to free speech online gets praise. So which should remain enshrined: freedom of speech or freedom from abuse?

How the law approaches free speech

Article 19 of the Universal Declaration of Human Rights (to which the UK became a signatory on adoption in 1948) declares that: "Everyone has the right to freedom of opinion and expression; the right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers." The argument goes that this includes protection for freedom of expression by the right to remain anonymous online.

The GDPR and the Data Protection Act 2018 give internet users the right to privacy and the right to withhold their personal details (from name to location) online.

When the free-speech line is crossed and becomes abuse, criminal law steps in. If an internet user suffers harm because of the activities of an anonymous (or a known) persecutor online, the police have powers to investigate those suspected of sending the messages – whether done anonymously or not. The Malicious Communication Act 1988 and the Communications Act 2003 make it possible to prosecute “trolling” – and many other forms of online harassment are also now covered by legislation.

If the police suspect criminal or terrorist activity, they have wide powers to investigate both the known and dark web (see What is the Deep Web? in the September 2015 issue of this Newsletter) and to arrest, detain and prosecute offenders. We all sleep better knowing this and few people object to these powers being granted to the police.

Are we ever really anonymous?

What has become clear since the Cambridge Analytica scandal is that there was a price for “free” internet and that we’ve given up more of ourselves than we ever intended to. As we have become constantly connected, none of us are as anonymous as we think. Browsing in private mode means cookies aren’t stored and no browsing history is logged on your computer – but that doesn’t stop other computers you are connected to from logging your activity or other applications on your computer monitoring what you are searching. Private browsing is never truly anonymous and even “going dark” will likely still leave a silicon crumb-trail all across the internet (see Tracking: your digital trail in the July 2018 edition of this Newsletter).

Government intervention

There have been famous cases where state authorities have asked tech companies to hand over data and been stone-walled. Perhaps the most famous instance of this is Apple, who refused to unlock the phones of the San Bernadino terrorists who killed 15 people in a mass shooting in December 2015. Apple refused a request from the FBI to add an operating system that would allow an infinite number of passcode attempts to be entered until the right one was selected. Their view was that it would compromise security of millions of Apple device users. At the time most people agreed they would not be comfortable with any government having what amounted to a digital skeleton key to their lives, but does that still feel right?

Flash forward a few years though and, in 2018, the then Digital Minister Margot James promised that new legislation requiring people to register their identity when using the internet would be tabled “at the earliest opportunity after Brexit.” This proposal was in response to a general public perception and acknowledgement
that people are emboldened in their opinions online, that cyber-stalking/bullying and overall abuse has risen and that voluntary codes are not effective. We are entitled to know who we are dealing with on the internet and to know who is calling us out, shouting us down or just shadowing us. The main issue with requiring people to register their identity when using the internet is that anyone with criminal intent is unlikely to give correct details and this type of “online passport” might just result in “fake online identities” being purchased. As of writing, we have no further details on this and it seems unlikely that it will top the Governments’ agenda any time soon, though it probably remains the best deterrent against trolling and bullying by the general public.

**Changing landscape**

What does seem apparent though is that the landscape around what is considered permissible and acceptable online is shifting. One indicator of this is that in September 2019 Facebook pronounced that it was a publisher (whilst defending itself in a lawsuit brought by Laura Loomer) and thus had a right to express its own opinions by blocking what it considered to be extreme views. This is a complete U-turn in policy because, as a publisher, Facebook can be held liable for allowing publication and reproduction of content published on its platform and it opens the business up to potential claims stretching back years. Enabling itself to act as judge and jury of content on its site, Facebook has said it will establish a de facto court for complaints … a difficult position to balance and one which will inevitably cause concern about it being both a regulator and regulated entity.

Might Facebook’s new “curated” approach to content limit the information we have access to? Concern already exists that Facebook and similar social media platforms act as echo chambers that validate opinions we already hold – fuelling precisely the type of extreme views that Facebook says it has a right to edit. Might this new position simply result in more fake news? George Orwell presciently realised that if citizens don’t know what is true and what is false, they can’t make a judgement about what to object to in their lives.

**Where does this leave anonymity?**

There are genuine public safety concerns around the ability for people to remain hidden online. With every heart-breaking tale of cyber-bullying or grooming and the massive rise in cybercrime as a whole, Governments have to step up and step in and it is clear that there will have to be a move away from anonymity to address these concerns. This debate is much like the current one around “burner phones” and the call to verify ones’ identity before buying a phone; honest people will do so, dishonest people will not and, if they are compelled to, the information they give will almost certainly not be true and this will also be the case with online identity verification.

There are already innumerable platforms that verify identity – some using blockchain to provide immutability and others drawing on verified sources to create a “wallet” or online passport and which could easily be adopted by everyone online. In this respect the technology industry is already finding workable solutions for these problems and if there is a groundswell of public adoption of such programs, it is likely that this type of positive action will be far more effective than law and regulation which quickly becomes obsolete or outmoded. It may be even more relevant to call for verification of identity and origin of information as we move into a world where our reality is digitally augmented and we need clear markers of what is actual and what is virtual.

**Further reading**

- New York Times: Anonymity May Have Killed Online Commenting [https://nyti.ms/2ObVdve](https://nyti.ms/2ObVdve)
- Financial Times: When online anonymity is a good thing [https://on.ft.com/3aQrlyt](https://on.ft.com/3aQrlyt) (paywalled)

Joanne Frears is IP & Technology Leader at Lionshead Law, a virtual law firm specialising in employment, immigration, commercial and technology law. She advises innovation clients on all manner of commercial and IP matters and is a regular speaker on future law.

Email j.frears@lionsheadlaw.co.uk, Twitter @techlioness.

Image by kalhh from Pixabay.
Introducing ICLR&D

By Paul Magrath and Daniel Hoadley

The most significant recent development at ICLR has been the launch, in March 2019, of our legal information lab, ICLR&D (research.iclr.co.uk).

This was conceived as a space where ICLR, whose traditional role has been publishing legal information built around primary source materials such as case law and legislation, could experiment with case law data in fundamentally different ways. The launch of ICLR&D was to some extent itself a form of experiment. The results have been interesting.

ICLR&D is not a product. Nor is it a physical laboratory or studio. Rather, it is a process or state of mind born of a conscious decision to harness our technical imagination, and to expand our development horizons, to embrace new ways of working with the data we already have, and to engage and collaborate with others in the legal information world.

That decision to create the lab was born of a growing awareness of the explosion of interest in the intersection between law and technology. Until now, however, what is often referred to as “legaltech” or “lawtech” seems to have focused its attention mainly on transactional legal content or processes, such as contract drafting, document discovery and regulatory supervision, or the development of chatbot apps and other public-facing products, and (with some exceptions) rather less on primary legal source material.

We felt that the legal information space warranted further research, and that ICLR was in a good position to do this. We identified four main areas of research, for each of which we created a separate project.

Blackstone

This project is concerned with the automatic enrichment of unstructured legal text using rules-based and predictive techniques. To date, it is the most developed of the ICLR&D projects, with a prototype being launched over the summer of 2019 and presented for discussion at international legal conferences during the latter part of the year.

The project’s deliverable is an open source piece of software, the Blackstone library and statistical model, that allows researchers and engineers to automatically extract information from long, unstructured legal texts (such as judgments, skeleton arguments, scholarly articles, Law Commission reports, pleadings etc). Trained using machine learning processes based on a body of existing case law data, it uses natural language processing (NLP) to parse raw text and to recognise named entities (such as case names, citations, provisions) and text categories (such as axioms, conclusions, issues), which can then be tagged accordingly and used to build analytical tools and visualization models based on the data.

That’s a simplification. Blackstone was developed using a single Python library called spaCy. The training data comprised the entire archive of ICLR’s law reports and unreported judgments. This corpus of content was broken down into single sentences, and then each sentence broken down into words. The words were then tokenised, vectorised, and parsed for parts of speech and dependency relationships within their respective sentences. The Named Entity Recogniser was trained on this data to spot the entities concerned, to pick them out of a mass of words and phrases, and tag them accordingly. Errors were corrected, and correct recognition was affirmed in a (manual, human) review process. Once the performance reached an acceptable standard, it could be applied to live, raw data. It could take a piece of legal text, analyse it, and pick out the named entities. A similar process was applied to words, phrases and sentences that carried particular types of meaning, such as the identification of an issue, the laying down of a rule, or the declaring of an axiom.

Such techniques are not new, even in the legal sphere: they have been developed in order to analyse the language of contracts or to classify documents for the purpose of discovery (disclosure) in litigation. So far as we are aware, however, Blackstone’s open source posture and focus on case law makes it the first model of its kind.

So that’s where we are. What was released last summer was essentially a prototype, a proof of concept. We are now working on a better, perhaps Beta, version. Watch this spaCy.

In the meantime, for the benefit of those who are not geeks, we have built an app which offers an easy (code-free) interface for the processing of ingested documents or extracts of text, using the Blackstone library: https://blackstone-demo.herokuapp.com.

Friction

This project looks at the promotion of open access to case law by analysing and mapping the judgment supply chain. On this project we have been working with the courts, publishers (such as BAILII and Justis) and providers (such as JUST:transcription) in an effort to improve the volume and speed of publication of both written and oral judgments.

Raconteur

This is concerned with exploring ways to accurately impart the significance and meaning of legal materials to the public. As an educational charity, ICLR sees public legal education as a priority, and one that can be addressed in other ways than the free supply of reliable judgments and case summaries in front of a paywall. Although this project remains in its infancy, a good example of what we envisage is the building up of free reference resources on the Knowledge section of ICLR’s website.

Endless Blue

This is a conceptual project focused on modelling the connections between the various sources of English law. In particular, it is concerned with understanding how cases relate to each other, using data modelling and visualisations to analyse the content and not merely the labelling of the cases and to find connections and proximities between them that may bypass more traditional forms of indexing and categorisation or subject matter classification.

Also published, fully linked, at www.infolaw.co.uk/newsletter
Collaboration is key

The driving philosophy of the lab is that open is better than closed. We want to work with others rather than pursue these projects in isolation inside a vacuum. So, if you have the urge to get involved with the lab or have an idea you’re interested in that you feel fits with our mission, we’d strongly encourage you to make contact with us.

Paul Magrath is Head of Product Development and Online Content at ICLR.
Email paul.magrath@iclr.co.uk, Twitter @maggotlaw.
Daniel Hoadley is Head of Research at ICLR.
Email research@iclr.co.uk, Twitter @DanHLawReporter.

Regulating the internet
News from Alex Heshmaty

Content moderation oversight board proposed by Facebook

Social media companies have traditionally argued that they are merely internet platforms as opposed to publishers with the ensuing editorial responsibilities (despite the odd court case where it has been to their advantage to hold themselves out as publishers). But in the face of increasing public controversy about malicious content plaguing social media sites, the Silicon Valley giants are being forced to take action to minimise reputation damage.

Facebook claimed that it had removed 1.5 million copies of the video of the New Zealand terrorist attack in the first 24 hours alone – which provides some idea of the scale of the challenge involved with content moderation.

Despite growing calls for urgent government regulation to set out the rules and responsibilities regarding harmful online content – including from Facebook supremo Mark Zuckerberg – when it comes to moderation decisions, social media companies are still largely self-regulating. They each appear to have their own set of individual guidelines as to what can and cannot be published on their platforms – eg. Twitter recently imposed a worldwide ban on political advertising, whereas Facebook ruled out such a ban on its own network. Enforcing their own guidelines is a challenge in itself; although much of the content moderation is automated, a significant amount of processing still needs to be done by humans (around 15,000) who can suffer psychological trauma as a result of having to routinely view distressing material as part of their job.

In December 2019, Facebook announced that it would create a court-style “oversight board” made up of 11–40 independent members, whose job would essentially be to rule on content which should and should not be allowed on the world’s biggest social network of 2.45 billion users. The charter has already garnered criticism from various quarters, but currently the company plans to make the board operational in 2020.

News publishers questioned about data deals with Google

As part of an investigation by the European Commission into the effect of data collection practices by Facebook and Google upon competition, news publishers have been sent detailed questionnaires regarding data sharing agreements with Google. In particular, the questionnaires seek details from publishers on ways in which the search engine behemoth uses data collected from their websites to track user activity, eg:

“Describe any agreements ... based on which Google collects data from your company or is allowed to obtain data from users of your websites or apps.”

The fear is essentially that Google could potentially be abusing its market dominance in terms of how it presents search results for news and how it runs its advertising services. One of the concerns seems to be that news organisations may be essentially “forced” to share their data in order to retain their rankings.

Meanwhile the Competition and Markets Authority (CMA) is conducting its own study into online platforms and the digital advertising market in the UK. A response by the European Publishers Council (EPC) warned that:

“While digital advertising should have created new opportunities for news publishers, the reality is that a very large part of digital advertising revenues has been captured by online platforms and, in particular, Google and Facebook (which commentators have referred to as an online advertising duopoly). This means that despite the resources they devote to producing original content, news publishers only receive a small fraction of the online ad investment made by advertisers.”

This investigation into competitive practices is part of a broader pattern of European governments and institutions attempting to regulate the international reach of Silicon Valley. We previously mentioned GAFA tax which will introduce a 3 per cent tax on digital services gross revenue made in France. Despite objections from the US administration and threats to retaliate with tariffs of up to 100% on imports of certain French products, Cédric O, the French junior minister for digital affairs, has confirmed that France will proceed with proposed tax.

Image by Tumisu from Pixabay.
See You Out Of Court

See You Out Of Court at buzzsprout.com/815344 is a new podcast focusing on new ways to resolve disputes without burning vast amounts of money through the courts. The podcast will inform you of all the options to resolve disputes without going to court, whether mediation, arbitration, adjudication, ombudsmen schemes and, importantly, by the parties themselves.

One theme throughout will be how technology is designing and offering more effective, practical, speedier less costly and therefore more accessible ways to resolve disputes and in this way to experience justice.

Each podcast will feature new developments with interviews with experts in the field. It will be of interest to mediators, arbitrators, lawyers, any organisation such as insurance companies or others who deal with claims and disputes and of course the general public.

See You Out Of Court is produced by Graham Ross, a lawyer and mediator who has been heavily involved in technology developments in ADR and ODR for over 20 years.

Graham has also set up a new panel of mediators at SeeYouOutOfCourt.com.

The end of a brand

In November 1999 Simmons and Simmons launched elexica.com, intended as “a gateway to the firm’s expertise for clients and law students, as well as a forum for the whole of the legal profession to discuss relevant issues in law” (my words at the time).

Elexica won plaudits and major awards, standing out in the early days as a model of how a large firm could showcase its expertise to clients.

In 2006 elexica was integrated into the Simmons and Simmons website and in 2007 Editor Mary Loosemore wrote for us in the Newsletter about the benefits:

“Back in 1999 we wanted to move into online services with a slightly different approach from that taken by other firms. We wanted to send out a message that we were forward thinking, not afraid of technology and able to work in an innovative way.

Technology and the market have changed significantly since then [and] elexica has evolved as the vehicle for getting our know how to clients and contacts. ...

As a result of these developments, Simmons & Simmons’ online offering is now more streamlined, giving clients and key contacts a seamless experience however they choose to consume our expertise.”

And so it remained for 13 years.

Then, in October 2019, Simmons and Simmons’ Twitter account excitedly tweeted, “Notice something different? We've been busy working with the best creative talent at [developers] to refresh our brand. Check it out: https://simmons-simmons.com #simmons #law #design”.

So I did.

I looked for elexica ... it had gone! There are no direct references to the former brand or its microsite. Traces do remain as there are internal links on the site to former elexica resources and these redirect to the equivalent pages on the integrated site. However, though a Google search for site:elexica.com lists 17,800 pages still in its index, all the links bar the default web address give a “404” on simmons-simmons.com – “Sorry, the page you are looking for can't currently be found.”

Despite my enquiries, I’ve not had an explanation. What a sad end to a once great site.

Out-Law.com

Not far behind elexica in the early web days was Out-Law.com from Pinsent Masons, launched in May 2000 to provide useful information to organisations and to showcase the expertise of Pinsent Masons.

Although no longer hosted at its own domain, Out-Law is still very much a fundamental aspect of Pinsent Masons’ web presence. Out-Law publishes over 2,000 legal news stories each year and maintains a few hundred legal guides.

Google still lists 26,500 pages at site:out-law.com but these all seem to redirect nicely to their new locations at https://www.pinsentmasons.com/out-law.
Law Via the Internet 2020

This year’s Law Via the Internet conference will be held on 15 and 16 September in London, hosted jointly by the Institute of Advanced Legal Studies, University of London, and BAILII and will focus on Legal Information and Access to Justice.

The Law Via the Internet conferences are organised under the auspices of the Free Access to Law Movement (FALM), a consortium of institutions dedicated to providing free and open access to law around the world.

Further information will be posted in due course at https://ials.sas.ac.uk/law-internet.

Online divorce

Online divorce is one of the key services being developed by HMCTS. It aims to deliver “a national end-to-end digital service for individuals and/or their legal representatives to make an application to legally end a marriage or civil partnership and resolve associated financial issues.”

The first stage for personal applications launched in April 2018. This enabled people to apply for an uncontested divorce, upload evidence and pay online. Since then more than 70,000 people have applied online, with 45,000 applying in 2019. More than 8 out of 10 users say they were satisfied or very satisfied with the service.

There is clear information and guidance on the whole process at www.gov.uk/divorce. HMCTS estimate it takes half the time to complete the online process as it did the old paper forms. Less than 1 per cent of online applications have been returned because of errors, compared to 40 per cent under the old system.

During 2019, acknowledgement of service and decree nisi applications were added to the online service and decree absolute digital applications were also released, completing the digital end-to-end service for unrepresented petitioners.

New scanning technology means that any paperwork sent in connection with online applications will be placed on the digital court file automatically. Following successful piloting, all legal professionals are now able to use the divorce online process, progressing through to decree absolute, on behalf of their clients. They can manage their accounts and view the progress of their client applications on a single dashboard.

In late 2019 consent order pilot testing began with 124 solicitor participants, and the end-to-end digital journey was put in place, with applications reviewed by 16 participating judges.

Solicitors receive automatic email notifications on key events and all orders are available to download.

... without tears

Online divorce service amicable.io does things differently. It exists “to help separating couples part ways on amicable terms, without spending thousands of pounds on lawyers.”

Couples complete a series of intuitive online forms and questions to reach agreement; their amicable “coach” writes up the agreement; and amicable’s legally trained specialists complete all the final paperwork.

The High Court was recently asked to rule on whether this model presented a conflict of interest. Mr Justice Mostyn gave a declaration that it did not and also went on to find that amicables’s role in preparing and submitting divorce documents did not amount to the conduct of litigation, nor did he believe the drafts which amicable helped prepare were within the scope of reserved legal instruments.

He concluded by saying that, “The declarations made in this case relate only to amicable. Other online divorce facilitators (and there are many) can only rely on them if their business models are virtually indistinguishable from amicable’s.”


Prof David Hodgson provides a detailed analysis of this judgment at http://bit.ly/2RSgb4z on LexisNexis Family Law:

“This is an important judgment for the benefit of online service providers and for the legal profession, as well as ancillary professionals such as mediators. … It will be for each organisation to ensure that their business model follows that approved by the court and that they do not breach either of the specific requirements. It will be a boost for the leading online service providers such as amicable providing affordable, yet high quality drafting and other family law services.

Nick Holmes is Editor of the Newsletter.

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

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

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