
Image: pbombaert / Moment / Getty Images

# Our Editorial Board look forward to the year ahead

2017 saw major data breaches, GDPR preparations, calls for stricter regulation of social media platforms, and overall, some substantial disruption by digital media companies, to name but a few topics. *Digital Business Lawyer* spoke to Members of its Editorial Board to gather concise expert insight into the key developments of 2017, and to paint a prospective picture of what we can expect to face in the year ahead.

**Rohan Massey, Partner at Ropes & Gray**

GDPR compliance programmes may have been the focus for most people in 2017, but the progress of the EC's proposed ePrivacy Regulation ('Regulation') also deserves some attention. The proposed Regulation has thrown up considerable issues regarding the alignment of ePrivacy and the GDPR as well as presenting challenges to many advertising and data related e-commerce business models. The desire to implement the Regulation along with the GDPR on 25 May 2018 may no longer be realistic, with the end of 2018 looking more likely. However, how the Regulation develops over the first half of 2018 will be important for all in digital business.

The Regulation remains in draft with several key issues still being negotiated between the European Council and Parliament. The interactions of the ePrivacy regime and the GDPR remain unclear, as does the thorny issue of how consent can be obtained for the purposes of the Regulation. Other points still in debate are those relating to the identification of direct marketing; who should be tasked with enforcement, noting that a Data Protection Authority's expertise may not extend to all areas of the Regulation; and the 'cookie' issue, with a ban on 'cookie walls' signalled as a priority by the EU Parliament.

Enhancing the current regime, the Regulation seeks greater clarity for users to know when their terminal equipment is accessed, including the use of cookies and other tracking techniques as well as on-device tracking. This is a particularly delicate issue as it goes to the core of many 'free' but data driven web business models as well as to the advertising businesses that may relate to them. There remains a desire to find a balance between ensuring proper privacy protection without undermining legitimate business models. However, it is likely that any balance will result in significant changes in the advertising industry, with consent a key issue for targeted online advertisements and the use of cookies. Privacy advocates support this and are offering up browser-based consent as a non-invasive solution, but the advertising industry see this as impractical based on both the limitations of technology and the need for granularity in consent, as per the GDPR, which would result in increasing numbers of people refusing to consent or to them losing the ability to even use websites and apps which require their consent. Whether the Regulation becomes a privacy albatross or a force for clarity and behavioural change depends very much on negotiations over the next 12 months.

**Gonzalo Mon, Partner at Kelley Drye & Warren**

In the world of social media advertising, 2017 was the year of the influencer. As consumers keep finding new ways to skip ads, companies keep finding more subtle ways to advertise. One of the fastest growing (and most cost-effective) ways to do this has been to use influencers. Companies will pay individuals with significant social media followings - or simply give them free products - in exchange for promoting those products.

The US Federal Trade Commission ('FTC') believes that when people see a product touted online, they have a right to know whether they're looking at an authentic opinion or an incentivised marketing pitch. Oftentimes, that requires a disclosure. Many advertisers and influencers feel that such disclosures dilute the authenticity of their messages, so they have either ignored the requirement or have made the disclosure in ways that the FTC feels are insufficient. The FTC stepped up its enforcement of influencer issues in 2017. In April, FTC staff sent more than 90 'educational' letters to companies and influencers, reminding recipients of their disclosure obligations. In September, they sent an additional 21 'warning' letters, asking recipients to explain what steps they planned to take to comply with the law in the future. This was coupled with the Agency's first settlement involving individual influencers.

As influencer marketing expands, we can expect the FTC to continue its enforcement in 2018. If you plan to use influencers, you need to take steps to ensure that your campaigns comply with the law. This often starts with an influencer agreement that (at a minimum) requires the influencers to make the necessary disclosures in a clear manner. But you can't stop there - you also need to take steps to monitor your campaigns to ensure influencers do what they're supposed to. Failure to do this can result in unwanted scrutiny.

**Michelle Cohen, Member at Ifrah Law PLLC**

Two words summarise digital business law in 2017: data breaches. Consumers continue to shop, bank and transact with businesses, and connect socially and professionally through websites and mobile apps. However, these interactions are often followed by announcements from these same organisations - such as credit agency Equifax and ride-

continued

hailing company Uber - that hackers accessed personal data improperly. High profile breaches dominated US and international news throughout the year, with no apparent end in sight for 2018. While some observers may say "that's nothing new," what is new are the companies involved, the sensitivity of the data compromised, and the questionable handling of the breaches. Despite receiving a warning from the US Department of Homeland Security, Equifax incurred the most high-profile breach in 2017, affecting approximately 143 million Americans (about half of all Americans). Equifax's breach exposed highly sensitive information, including social security numbers, birth dates, and home addresses. Equifax received widespread criticism for waiting over six weeks to disclose the breach. Uber faced numerous issues this year, including revealing that in 2016, hackers stole 57 million driver and rider accounts (and this is not Uber's first breach 'rodeo'). Uber paid $100,000 in ransom money to the hackers to keep the breach quiet. The subsequent revelation of the breach resulted in the termination of employment of several high-level Uber officials. Uber also faces investigation by several state attorney generals and numerous private lawsuits, including class actions.

Large data breaches have occurred with regularity over the last several years. However, Congress, regulators and the public are pushing for action and accountability. Congress quickly held hearings on Equifax's breach. Legislators have also proposed legislation requiring notification within 30 days of a breach, with jail time for officials who conceal a data breach. US federal law does not have a national standard but instead only imposes standards in certain 'sector-specific' industries such as financial services and healthcare. States vary in their approaches to timing data breach disclosures. After these recent debacles, it seems likely that Congress could actually move legislation to address failures to disclose breaches. Even in the absence of Congressional action, state attorney generals and regulators such as the Federal Trade Commission will continue to utilise their broad powers to investigate and take enforcement actions where companies fail to secure consumer data and fail to promptly report breaches. In summary, expect to see more enforcement actions, and larger dollar settlements to resolve those actions.

**Iain Connor, Partner at Pinsent Masons**

It may have passed you by, but in 2018 the UK will have a new law to protect trade secrets. Despite Brexit, the UK Government, along with all other EU Member States, has committed to implementing the EU's Trade Secrets Directive by June 2018. The Directive came into force in 2017 with an implementation date of 9 June 2018. So far, no Member State has passed legislation to give effect to it and so we are looking forward to seeing how this harmonising measure will be adopted. The Directive takes its basic definition of a trade secret from the TRIPS Agreement and follows the enactment in the US of the Defend Trade Secrets Act, which also adopted the TRIPS definition.

For digital businesses, the new Directive is potentially very useful as it will give an added layer of protection against the unlawful use of know-how which may or may not be capable of protection via intellectual property rights. A 'trade secret' is defined in the new Law as information which is:

1. Secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known or readily accessible to persons within the circles who normally deal with the kind of info in question;
2. Of commercial value because of its secrecy; and
3. Has been subject to reasonable steps by the person lawfully in control of the info to keep it secret.

The key question businesses need to be prepared to answer is whether they have taken 'reasonable steps' to keep information secret. In order to do this, businesses should identify and record their business know-how and ensure that there are policies and procedures in place to keep it confidential. If the information is then used without permission, businesses will have a host of remedies under the new Directive.

**Rico Calleja, Media Law Consultant at Calleja Consulting**

Data, data and more data. The current, not unwarranted, obsession with GDPR and its troublesome sibling, the proposed ePrivacy Regulation, has deflected critical gaze from other significant initiatives taking legislative form as part of the European Commission's Digital Single Market Strategy.

The Regulation on ensuring cross-border portability of online content services will apply from April 2018, allowing Europeans, in the Commission's words, "to fully use their online subscriptions to films, sports events, e-books, video games or music services when travelling within the EU." Political agreement on this Regulation on unjustified geoblocking was reached in November with the Commission saying that "by Christmas [2018] Europeans should be able to shop online without being blocked or re-routed." The final form of that Regulation is awaited with some interest as the EU Parliament's negotiators achieved "an ambitious review clause" requiring the Commission to assess, within two years after the entry into force of the Regulation, not only whether to extend its scope to non-audiovisual copyrighted content, but also "to carefully analyse whether additional sectors, such as the audiovisual and transport services, should be included in the scope."

The proposed Directive on Copyright in the Digital Single Market is also likely to rekindle debate, particularly with regard to the related right for press publications. The process of revamping the Database Directive may also get under way with the Commission keen to determine whether it is still relevant in view of the development of new technologies and new business models based on data exploitation. On the domestic front, alongside the Government's Internet Safety Strategy, the DCMS has formally proposed that the British Board of Film Classification be designated as the regulator for the age verification of online pornography under the Digital Economy Act 2017, with the intention that those measures will be in place in 2018. In the shadow of Brexit, the Government is consulting

**The proposed Directive on Copyright in the Digital Single Market is likely to rekindle debate, particularly with regard to the related right for press publications.**

on changes to the Investigatory Powers Act 2016 to align with the CJEU's ruling in joined cases C203/15 *Tele2 Sverige AB and Watson*, while at the same time consulting on a draft Communications Data Code of Practice, which sets out how the safeguards governing the retention of communications data by telecommunications operators and its acquisition by public authorities, including the police and security and intelligence agencies, will operate. The move is being seen as a reaction to a perceived threat to the UK's data protection adequacy status post-Brexit.

**Becket McGrath, Partner at Cooley (UK) LLP**

In terms of UK enforcement in the competition law sector, the most interesting case for 2018 is likely to be the appeal to the Competition Appeal Tribunal ('CAT') by golf club manufacturer Ping against the decision by the Competition and Markets Authority ('CMA') of August last year. That decision imposed a fine of £1.45 million on Ping for infringing the UK and EU law prohibitions of anticompetitive agreements by requiring authorised retailers to sell its clubs only following an in-store 'face to face' fitting and prohibiting online sales. In its appeal, which is due to be heard by the CAT in May 2018, Ping is challenging the CMA's reliance on EU law precedent stating that online sales bans are inherently illegal. The CMA's current crop of competition enforcement cases in the sector is smaller than it has been in recent years, being limited to one investigation into the use of 'most favoured nation' (or parity) clauses by price comparison sites selling home insurance. As this case was opened only in September last year, it is unlikely to reach a conclusion during 2018. The CMA nevertheless remains interested in competition in online and digital markets, which it identifies as a key theme driving case selection in its Annual Plan for 2018-19. That document also notes the creation of a 'digital, data and technology team' within the CMA and the Authority's particular interest 'in how companies use online data and the growth of algorithms in business decision-making, including price discrimination.' Whether this interest results in the opening of live enforcement cases in 2018 remains to be seen.

**Oliver Bray, Partner at RPC**

2017 was the year of digital disruption. Everywhere you looked digital was uprooting traditional models, with online platforms and new entrants alike capitalising on smarter ways of doing business. Uber may have grabbed the most headlines, but all industries began to feel the heat - for example, look at the power shift in sports, with Amazon Prime outbidding Sky for the rights to the ATP World Tour and Formula One's announcement of a global partnership with Snapchat. As ever, the regulators seem to be playing catch up - be it for control of influencer marketing (now a billion dollar industry) or their push for more active moderation of online content, as demonstrated by the introduction last October of a new German law, the Netzwerkdurchsetzungsgesetz (the Network Enforcement Act), which imposes huge fines on social networks if they don't delete illegal content within 24 hours of it being reported.

As for 2018, it's clear that the debate over the role and responsibilities of the online platforms will continue to rage as they grab an ever-greater slice of global business, whether in the explosion of live streaming or in the march of instant messaging, now set to take over from traditional retail channels as brands begin to explore more direct consumer relationships powered by chatbots and AI. But it's AdTech which is likely to face the biggest disruption, primarily because of the ePrivacy Regulation. The latest draft (released in October) pushes for more direct control over tracking cookies, including a ban on cookie walls, and in turn this would have extreme consequences for online behavioural advertising (the lifeblood of many sites). The seriousness with which AdTech must take this threat is evidenced in recent comments by MEP Birgit Sippel (the European Parliament's Special Rapporteur for the ePrivacy Regulation) when she said "What we are aiming at is to abolish surveillance-driven advertising." It all points towards a bumpy 2018 for digital, meaning that we (as digital lawyers) are going to remain very busy indeed.

**Nick Johnson, Partner at Osborne Clarke**

For me, as a UK advertising and online regulatory lawyer, the defining theme of last year was the GDPR. Although some organisations had already started preparing, it wasn't really until 2017 that many finally turned their minds to it. Some have inevitably left it too late to achieve anything close to full compliance by May 2018, and for some there will also have been a dawning realisation that the GDPR may fundamentally challenge existing business models. We also heard a lot about transparency in its various forms. *Guardian v. Rubicon* reignited industry debate about financial transparency, just as it seemed the ripples from the ANA's hard-hitting 2016 report were subsiding. As for transparency of commercial content, regulators got very interested in brands' use of online influencers, with a string of Advertising Standards Authority cases on the degree and type of advertiser control over influencers' posts and marketing communications. The distinction between marketing and editorial also came under ICO scrutiny in the *FlyBe*, *Honda* and *MoneySuperMarket* cases on re-permissioning emails.

Going into 2018, key issues will include:

1. Platform liability: With Germany's NetzDG now in force and political capital to be made from platform-bashing, expect more discussion about intermediary liability defences.
2. ePrivacy Regulation: Trilogue has still not started, so much is still up in the air. If the final version looks anything like the Parliament draft then the impact on the online advertising industry - and the internet economy generally - could be severe.
3. Class actions: An EU proposal on collective redress is expected. Is the 'Google You Owe Us' representative action a sign of things to come in the UK and Europe more generally?
4. AI: Expect to see regulators and businesses grappling with how to bake social responsibility measures into AI creation and targeting of persuasive personalised ad messages.