People, platforms and pipes – liability, blocking and law enforcement

This short paper — effectively speaking notes — accompanies Neil Brown's presentation to Informa's IT Law Summer School 2015, at Downing College, Cambridge. It is licensed under CC BY 4.0

Introduction

This note covers four areas at a very high level — given the time available for the presentation, it is inevitable that this is a light touch treatment of the area, and necessarily omits quite a lot of detail. Please use this as a starting point for further research.

For three of the areas, there is a reasonable degree of overlap: user liability for electronic speech, liability of online intermediaries and filtering and blocking in respect of pornography, copyright and trade marks.

The fourth area is law enforcement access to communications data.

User liability for electronic speech:

Is the Internet a regulated space?

John Perry Barlow wrote in his "Declaration of the Independence of Cyberspace"[1] that national laws had no application:

> "You have no sovereignty where we gather".

Later on, he says that:

> "anyone … may express his beliefs, no matter how singular, without fear of being coerced into silence or conformity."

That established legal principles do not apply in cyberspace.

If there is no law applicable to the Internet, and it is subject only to its own laws, I have wasted a lot of money on Internet law books.

It is, without doubt, a romantic idea of a cyberutopia, but not the reality of the world today.

It will come as no surprise to you that laws do apply online, but it is worth making that point expressly.

Slander / libel

As with many things that we might discuss under the topic of "Internet law", the most obvious example of the regulation of electronic speech comes through simply the application of existing, offline laws to online behaviours.

The laws of slander and of libel do not suddenly cease to apply when the speech in question takes place online.

The seminal case on this topic is one of the real stalwarts of Internet regulation law: *Godfrey v Demon Internet*, from 1999.[2]

The claimant, Godfrey, was a physicist. And someone pretending to be him sent a posting to a Usenet newsgroup, which was

---

[1] https://projects.eff.org/~barlow/Declaration-Final.html

[2] [1999] EWHC QB 244: http://www.bailii.org/ew/cases/EWHC/QB/1999/244.html

"squalid, obscene and defamatory". The newsgroup was carried by the defendant, Demon Internet.

Godfrey asked for Demon to remove the message but Demon did not, although, technically, it could have done so, and the post remained available under it expired. A period of 10 days or so.

Demon attempted to make a defence that it could not be liable for this third party posting but, on an interim application to strike-out, the High Court held that:

a.) Demon did "publish" the posting, and that

b.) they could not rely on the defence of "not knowing" that they contributed to the publication of a defamatory statement.

The case then settled.

In the case of *Smith v. ADVFN*,[3] in 2008, Eady J addressed the issue of whether a posting on a bulletin board should be treated as slander or libel.

At paragraph 16, he commented that the transient nature of online debate on bulletin boards is closer to slander:

> "When considered in the context of defamation law, therefore, communications of this kind are much more akin to slanders (this cause of action being nowadays relatively rare) than to the usual, more permanent kind of communications found in libel actions. People do not often take a "thread" and go through it as a whole like a newspaper article. They tend to read the remarks, make their own contributions if they feel inclined, and think no more about it."

Someone claiming slander, of course, will need to prove that they have suffered financial loss if it did not relate to their professional capacity, rather than merely reputational damage.

---

[3] [2008] EWHC 1797 (QB): http://www.bailii.org/ew/cases/EWHC/QB/2008/1797.html

But slander is not the way things have gone. In the high-profile case of *McAlpine v Bercow*[4], McAlpine claimed that Bercow's Tweet:

> "Why is Lord McAlpine trending? *Innocent face*"

was libellous.

Bercow disagreed, although acknowledged that it was probably not the smartest thing to post.

Tugendhat J, in the High Court, held that:

> "the reasonable reader would understand the words "innocent face" as being insincere and ironical. There is no sensible reason for including those words in the Tweet if they are to be taken as meaning that the Defendant simply wants to know the answer to a factual question."[5]

Moreover, her Tweet meant:

> "in its natural and ordinary defamatory meaning, that the Claimant was a paedophile who was guilty of sexually abusing boys living in care."[6]

The case was settled out of court but, in the eyes of this judge, at least, a Tweet can be actionable as libellous.

What about those who retweet things? Is that an act of publication, of endorsement? Currently untested, although many Twitter users, including lawyers, explicitly declare that their retweets are not endorsements, as if the default position is that they are.

Trolling / bad jokes

Moving from the civil to the criminal.

You'll probably remember the unfortunate case of Paul Chambers, the traveller who Tweeted his frustration about the potential

---

[4] [2013] EWHC 1342 (QB): http://www.bailii.org/ew/cases/EWHC/QB/2013/1342.html

[5] Paragraph 84

[6] Paragraph 90

closure of his local airport in words that were perhaps not particularly wise.

Chambers was prosecuted under s127, Communications Act 2003.

He was convicted at first instance, and the conviction was upheld on its first appeal, but overturned on appeal to the High Court. In this case, the judge held that:

> "If the person or persons who receive or read it, (the message) or may reasonably be expected to receive, or read it, would brush it aside as a silly joke, or a joke in bad taste, or empty bombastic or ridiculous banter, then it would be a contradiction in terms to describe it as a message of a menacing character."

CPS charging guidance reflects that "it is more appropriate to charge bomb threats" under s51, Criminal Law Act 1977, which deals specifically with bomb hoaxes.

And while Chambers' conviction was overturned, others have been imprisoned for their Tweets. A man Tweeted rape threats to MP Stella Creasy, following her support for putting Jane Austen on the £10 note. He was prosecuted, found guilty under s127, and jailed for 18 weeks.

As I said at the beginning, these are not new legal frameworks. Online speech is fundamentally the same as offline speech, and liability for that speech falls just as it does for offline speech. There are certainly issues that what once might have been a private conversation may now be played out on a platform which is actually visible to anyone in the world, but the underlying principle is that liability for speech does not change fundamentally simply by taking place online.

Laws v. platform AUPs and code controls

As a brief aside, it is not just law in the sense that we, as lawyers, tend to understand it which regulates online speech. When you engage in an activity on a third party's platform — such as Facebook or Twitter — that person controls the environment in which you operate.

They are likely to have their own platform framework for acceptable content — their acceptable use policy, for example, or community standards — and probably reserve the right to take

action, such as deleting content, banning a user or even permanently deleting a user's account, for breach of those guidelines.

As well as legalistic policies, they may also control the environment through code. If they have coded their platform to delete all posts referring to, say, Taylor Swift, you are limited in your speech notwithstanding the position at law.

Lessig called this the difference between regulation by East coast code — law — and West coast code — software. Free speech is limited by the tools available to you.[7]

[7] His book, Code 2.0, is well worth a look.

Liability of online intermediaries:

To what extent should intermediaries be liable for the content posted or viewed by their users?

This area is, perhaps inevitably, an issue of freedom of speech, often balanced with right to property (which includes intellectual property).

eCommerce directive

The key to understanding the eCommerce directive and the rules on intermediary liability is that the framework exists to ensure that incentives are set correctly, to encourage the development of new and exciting online platforms:

> (40) Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities"

Providers of services which simply enable third parties — users — to act in a particular way should not be responsible for users' actions. However, where a service provider colludes with a user in doing something, they cannot expect to be shielded from liability:

> (44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of 'mere conduit' or 'caching' and as a result cannot benefit from the liability exemptions established for these activities.

The UK implemented the eCommerce directive through the eCommerce Regulations 2002.

There are three shields of liability under the eCommerce Regulations

- Mere conduit
- Caching

- Hosting

I'm going to discuss "mere conduit" and "hosting", as those are the most interesting and relevant.

Mere conduit

The mere conduit shield is designed to provide protection for those providing connectivity services: those providing services which "consist in the transmission in a communication network of information provided by a recipient of the service."[8]

This is with the provisos that the communications provider does not start the transmission, select the receiver of the transmission, or select or modify information contained in the transmission.

Hosting shield

The hosting shield applies to those who provide an "information society service, which consists of the storage of information provided by the recipient of the service".[9]

Like Article 12, there are provisos: the service provider must not have "actual knowledge" of illegal activity, or "information … from which the illegal activity … is apparent" or, if they come into possession of such knowledge, they act "expeditiously" to remove or disable access to the information.

No general obligation to filter / monitor

The eCommerce directive expressly provides that Member States are not permitted to impose a general obligation on providers to monitor the information which they transmit or store,[10] although each of Articles 12 and 14 provides that they do not affect the possibility of a court in a Member State issuing a provider with a court order to terminate or prevent an infringement.

---

[8] Article 12, directive 2000/31/EC

[9] Article 14, directive 2000/31/EC

[10] Article 15, directive 2000/31/EC

ISS v ECS

I'd like to flag something for you to ponder on, particularly in the context of something I suspect Mike will talk about later. And that is the definitions of "Information society service" and "electronic communications service", in the context of the mere conduit shield.

The shield applies to providers of "information society services", and recital 18 to the directive talks in terms of:

> "span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line;"

The definition of "information society service" goes a bit further back in regulatory history, to the technical standards directive, of 1998, as amended. And this provides that an information society service is:

> "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

It is something — a service — which is provided remotely.

Dive into the communications regulatory framework, though, and you find a number of other definitions, including that of "electronic communications service". And an "electronic communications service" includes:[11]

> "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks"

Further:

> "it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;"

What does Article 12 — mere conduit — say? That it applies to someone providing the information society service which "consist[s] in the transmission in a communication network of

---

[11] 2002/21/EC, at Article 2(c)

information provided by a recipient of the service". That sounds like an electronic communications service to me.

Does someone who provides an end user with an Internet connection provide an electronic communications service, or and information society service, or both. Can something be both an electronic communications service and information society service, or does this language mean that they are exclusive?

The shield of liability under mere conduit is designed to protect those providing Internet access services. But, to me, those feel closer to electronic communications services than information society services.

Specific defamation rules

Recently, specific legislation has been introduced in respect of defamation, and a shield of liability existing specifically in respect of slanderous and libellous material. The changes are, according to the Ministry of Justice, to

> "rebalance the law on defamation to provide more effective protection for freedom of speech while at the same time ensuring that people who have been defamed are able to protect their reputation."[12]

The rules are embodied in s5, Defamation Act 2013, and the Defamation (Operators of Websites) Regulations 2013.

The schedule to the Regulations sets out the actions which an operator must taken in response to a notice of complaint in order to maintain their s5(2) defence. There is a Ministry of Justice guidance document available, along with nine pages of frequently asked questions, which probably tells you how complicated the rules are.[13] Fine for hosting providers with lawyers at their disposal, but probably not so great for the myriad of individuals running their own blogs and websites.

---

[12] "Complaints about defamatory material posted on websites: guidance on section 5 of the Defamation Act 2013 and Regulations" (January 2014), Ministry of Justice.

[13] Available from https://www.gov.uk/government/publications/defamation-act-2013-guidance-and-faqs-on-section-5-regulations

Filtering and blocking:

Sometimes, laws attempting to regulate user behaviours are considered insufficient. When this happens, laws are often used to impose obligations on technical intermediaries to bring about the desired result.

Think about the issue we discussed earlier: you are limited in terms of what you can do on Facebook by the functions and facilities that Facebook provides. You are limited by Facebook's code.

Where law is insufficient as a tool for influencing user behaviour, some may seek to force intermediaries to act. This is Lessig's theory: he who controls the code controls the user experience.

Pornography

Currently, there is no law in the UK which requires the filtering or blocking of pornography, but there is a lot of political pressure for doing this.

As such, all major mobile operators and, increasingly, fixed line operators, have implemented systems to enable subscribers to choose whether or not they wish for lawful pornographic content to be accessible via their connection.

For mobile, this is opt-out, in the sense that the block is in place by default, and a subscriber needs to request its removal. For fixed line services, it tends to be either opt-in, or else what is known as "active choice": a requirement that a subscriber makes a selection either way.

How many of you have seen this sign anywhere? Do you know what it means? It's the "family friendly Wi-Fi" sign, and it is designed to show that a public Wi-Fi service is filtered.

Although most of the recent debate has been about private connections, public connections too are of concern, perhaps more so. Should you be able to access pornography via a Starbucks or McDonald's Wi-Fi connection, for example? To an extent, this is a commercial issue — do cafe operators want patrons watching pornography if their shops? — but also a child protection one: even if parents are supervising a child's Internet use at home, if

they can easily access pornographic materials from any number of hotspots available in town, this may be of concern.

Indecent images of children

As with lawful pornography, there is no legal mandate in the UK that requires an Internet access provider to block access to illegal content: in particular, indecent images of children.

Many — most, but not all — access providers do so, on a voluntary basis, through a subscription to the Internet Watch Foundation's CAIC (Child Abuse Image Content) list, but it is not a legal obligation.

Copyright and trade mark infringement

Oddly, perhaps,[14] while there is no law on indecent images of children, the legislature has seen fit to provide a legal framework for forcing access providers to block websites which infringe, or encourage a user to infringe, copyright. And this approach has recently been extended to cover trade marks too.

From a copyright perspective, s97A CDPA 1988 provides a basis for a judge to order an ISP to block access to sites which infringe copyright, or which encourage a user to infringe copyright.

Generally, a representative of the copyright industry will try to agree a form of court order with the intermediary in question, and then take it to the High Court — to date, mostly Arnold J — to have it ordered.

Perhaps the most famous judgment in this area is that in respect of The Pirate Bay,[15] although orders have also been granted for approximately 47 sites.

The order will tend to set out to the ISP to which the order applies, the steps which that ISP is required to take, and a schedule of the sites to which the order applies. As a result of interventions by the Open Rights Group, operators are generally now required to put up a holding page, explaining to a would-be

---

[14] Or perhaps not so oddly, if you consider the lobbying power of the copyright industry.

[15] *Dramatico v. BSkyB* [2012] EWHC 268 (Ch): http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html

visitor why the site has been blocked. Worryingly, they tend to give the copyright industry the right to update the list without seeking a further court order.

In the recent case of *Cartier*[16], website blocking orders were extended to sites which infringe trade mark rights. In this case, Arnold J held that not only could copyright law extend to covering trade marks, but that general law — s37(1), Senior Courts Act 1981 — would also permit such an order to be made, since it is very broad in the discretion it grants a judge.

This outcome is not wholly surprising, given the CJEU's ruling in *L'Oreal v. eBay*[17]. In this case, the CJEU held that a provider of online services, such as an auction platform, fell within scope of the mere hosting provision of the eCommerce directive, but that an order could be made by a national court requiring them to curtail current infringements and prevent future infringements. Any injunction must, however,

> "be effective, proportionate, dissuasive and must not create barriers to legitimate trade." (para 144)

There is an ongoing issue of costs: who should bear the costs of seeking orders for blocking, and the costs of implementing and operating blocks. Unsurprisingly, ISPs tend to argue that it should be for rightsholders, and rightsholders claim that it should be ISPs. We wait for the outcome of the appeal in *Cartier* for clarity on this.

Does filtering / blocking work?

There is debate as to whether blocking actually works, and, indeed, what is "good enough". Rightsholders probably start from the position that anything which makes infringement more difficult is a good thing, even if not wholly effective, and that ISPs should be burdened with increasingly restrictive obligations under the problem is cracked. Those intent on circumventing blocks can probably do so trivially, given the easy of setting up a virtual private network to a less-restricted country. Arnold J

---

[16] [2014] EWHC 3354 (Ch): http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html

[17] C-324/09

speaks in *Cartier* in terms of a blocking order having just "some dissuasive value".[18]

There is also the potential "Streisand" effect: making a fuss about something might simply result in further awareness of it, rather than just letting it go quietly.

Lastly, no filtering / blocking system is perfect, and most systems will, at some point, result in either (or both) over-blocking, restricting access to more than they should, or under-blocking, allowing access to sites which should be blocked. Over-blocking has ramifications for freedom of speech and freedom to do business, unless there is a very quick way of resolving the issue.

One area in which there is relatively little written is the question of liability. If an ISP includes within its block list a site which, as a matter of fact, should not be blocked, should they be liable to the site's operator? Under the tort of negligence, that does not seem a stretch. But perhaps there is a public policy defence that, based on the state of the art and reasonable cost, some degree of over-blocking is inevitable.

What happens if a provider offers a content filter, to prevent a child's access to pornography, and something slips through the net? Is that negligent? Is there any harm? Is it something simply to be handled in the subscriber's contract or does it go to the heart of whether the blocking service is fit for purpose?

---

[18] Paragraph 238

Law enforcement access to communications data:

I have been asked to touch briefly on the issue of access to communications data by law enforcement. And, as I said at the beginning, the issue of surveillance of communications is not something which can be readily covered in the five minutes or so I can allocate to it. So this is very much at a high level.

In the aftermath of the 7/7 bombings in London, there was considerable political incentive to pass a directive which granted Member States the ability to order communications providers to retain metadata relating to the communications which they carried over their networks. This is the who, when and where, and not the content of the communications.

The data retention directive was held to have been invalid *ab initio* by the European Court of Human Rights in 2014, in a case brought by the Irish digital rights group Digital Rights Ireland.[19] The gist of the ruling was fundamentally that, as written the directive's interferences with the fundamental right to respect of one's communications were disproportionate, for a number of different reasons.

In 2014, the UK government introduced legislation, which was to be passed as the Data Retention and Investigatory Powers Act 2014, which fundamentally replicated the framework under the European directive, albeit with a number of tweaks, in particular to do with extraterritoriality, and adding some additional safeguards to the access of communications data. DRIPA, as it inevitably become known, was supplemented by the Counter-Terrorism and Security Act 2015, which extended the categories of data which providers can be ordered to retain to include certain Internet activity data, designed to enable law enforcement to link an IP address with a subscriber.

The framework for accessing communications data remains largely unchanged, in the form of Chapter 1 Part II of the Regulation of Investigatory Powers Act 2000. This enables certain law enforcement agencies to require communications providers to hand over communications data, with an internal governance procedure for the granting of authorisations. One of the changes brought in by DRIPA was a prohibition on the use of non-DRIPA

---

[19] *Digital Rights Ireland*, joined cases C-293/12 and C-594/12

legislative bases for accessing communications data retained under a retention notice, unless by means of a court order.

For more information on this, and for a taste of the way things might go in this area, I would highly recommend reading David Anderson QC's recent publication "A Question of Trust", which explores is some considerable detail the nuances of the legislative framework around communications surveillance generally, and makes some proposals for reform.

Last minute note: the High Court held on 17th July 2015, following a request for judicial review by MPs David Davis and Tom Watson that s1 DRIPA is "inconsistent with European law", and granted an order for disapplication, suspended until 31st March 2016.[20] *The government has indicated its intention to appeal.*

[20] [2015] EWHC 2092