Cyberspace and the Law

The Bar Association for Commerce, Finance and Industry's Denning Lecture 2015[1]

Lord Reed

24 November 2015

It is sometimes said that Tesco know when one of their female customers is pregnant before she does. If she uses a Clubcard, her sudden craving for pickled onions, or whatever else it may be, is noted and interpreted by their software.

That may or may not be apocryphal, but I was told what is certainly a true story by an American judge who recently married. When his wife changed her name on her Facebook account, she was immediately bombarded with online advertising by divorce lawyers. The software noted her change of name, worked out the possible explanations, which presumably included separation from a husband, assessed the consequent commercial opportunities, and provided the relevant marketing services to third parties. And you will all know that if you browse online for, say, a shirt, you will then find advertisements for shirts whenever you log on for the next few months.

The way in which Internet technology turns those of us who use it into products, as we are induced to provide information about ourselves online, often unconsciously, which is gathered by cookies and then sold on to advertisers, is of course not its only important consequence. It has resulted in a more profound cultural change. From prehistoric times until the relatively recent past, men and women encountered each other face to face. What they knew about each other was what they could remember. Then they began to write letters, and more recently to read newspapers. Information could

[1] Delivered to the Bar Association for Commerce, Finance and Industry at Inner Temple on 24 November 2015.

then be recorded and stored in archives of one kind or another, to which some people at least could obtain access. If they devoted a lot of time and effort to it, and if they knew what they were looking for, they might be able to find out information about a person's past from searching, for example, through a newspaper archive. But in general they used to forget, or if they remembered they usually couldn't prove it, at least without great difficulty. That situation, equally familiar to the Ancient Britons as to our parents or grandparents, has changed completely. Search engines, social media, and digitised archives have changed our knowledge of each other beyond recognition.

The Internet is now probably the primary means by which information is communicated around the world, and access to that information is of immense commercial value. It can raise legal issues of all kinds, including fundamental human and constitutional rights. The legal regulation of the Internet is a very large subject which we have only just begun to explore in litigation. Some of you will know much more about it than I do: I make no claim to be an expert in this area.[2] It is however something which affects us all, and which is bound to be of growing legal importance.

So I thought I might try this evening to consider, at an elementary level, a few of the issues that have come before the courts to date, the courts' responses, and some of the implications for the future. I'm not going to address public law issues concerning such matters as surveillance of emails and other computer usage by the police and the security services, or criminal law aspects of the use of the Internet. I'll focus on issues arising as between individuals or companies and the providers of online services. And in the time available, I can only scratch the surface. I don't propose to consider the substantive law governing the transfer of information by means of the Internet, such as the law of defamation, intellectual property law, confidentiality, privacy and data protection, on which there is now a substantial amount of case law, but will focus instead on more general and fundamental

[2] An account of the history of internet governance is contained in Goldsmith and Wu, *Who Controls the Internet: Illusions of a Borderless World* (OUP, 2006).

questions about jurisdiction and remedies.

At one time, the Internet was heralded by some people as a medium which transcended territorial boundaries and was therefore beyond the control of national governments. It was regarded as presenting an opportunity for a new kind of politics, democratic or anarchic according to taste, and a new kind of freedom of speech, regulated, if at all, by the self-government of the online community. Neither private law, nor public law, nor criminal law controls were thought to be capable of practical application. Some commentators continue to argue that the Internet should be self-regulated. It does of course have important elements of self-regulation, both by the market and by social norms; but, as you might expect, national and international authorities have been reluctant to accept that external regulation is not also required. Furthermore, Internet companies have discovered that they are themselves reliant on national legal institutions in order to maintain their commercial operations: they rely as much on intellectual property law, contract law and so forth as more traditional types of enterprise.

The idea that the Internet lies outside the proper scope of territorial regulation is encouraged by the language that we use. We speak of "the web", and of "cyberspace": expressions which suggest that the Internet exists in a realm which is virtual or non-geographical, rather than in locations that we can point to on a map. There is an element of truth in that: language of that kind does reflect an important aspect of the Internet, which I will come to in a moment. Nevertheless, it is ultimately misleading.

It is misleading because it fails to reflect the basic nature the Internet, as an international communication system which links computers, or networks of computers, and enables information to be transmitted between them. Those computers have physical locations in the real world. So do the people using them. So do the Internet service providers or ISPs who provide access to the Internet to most of its users, and who host webpages. And it is possible to locate where they are: for example, the

names and addresses of holders of domain names and IP addresses are registered in a publicly accessible registry, under requirements imposed by a private organisation, the Internet Corporation for Assigned Names and Numbers. They can be obtained by carrying out a who.is Internet search. So, in principle, the people using the Internet, in one capacity or another, are susceptible to the jurisdiction of national authorities and national courts.

At the same time, the non-geographical language of "cyberspace" reflects another important aspect of the Internet. It is not like a postal system or a telephone system, where information is transmitted directly and in a readily identifiable way from a person in one location to a person in another. The communication of information via the Internet normally involves a number of computers, which may be scattered across the world. The information itself is delivered in packets: that is to say, it is broken down into the pieces of a jigsaw, as it were, which are then sent by different routes, with the same piece of the jigsaw often being sent simultaneously by a number of different routes. Each computer which receives a piece of the jigsaw copies it, discards the piece it received, and forwards the copied piece to a number of other computers for further onward transmission. This fissiparous and opaque technology reflects the Internet's military origins, and the need for the system to be capable of withstanding the destruction of large numbers of the component computers. So the links in the chain, and their physical location, are not obvious except to themselves.

One consequence of this technology is that one has to be careful, when applying legal concepts and statutory provisions, to consider in what sense one can say that an image or a document is transferred from, say, a website to a person visiting the website. It is no accident that legislation dealing with the Internet focuses on the transfer of information or data rather than the transfer of documents. Another consequence is that locating where information is at a given moment during the process of communication is practically impossible. Indeed, a single website, or even a single webpage, may in reality be formed from a number of different pieces of information held on different computers, which

may be located in different jurisdictions. And the owner or operator of the computer, or network of computers, may be in another jurisdiction again. A third implication of this opaque technology is that it may in practice be unrealistic to base legal conclusions on the location of the computers used in the course of Internet transactions.

The fact that the use of the Internet often involves a number of different jurisdictions, and is geographically opaque, raises obvious problems in applying some of the fundamental concepts of private international law. Our law in relation to jurisdiction, for example, relies heavily on our ability to determine where an act or event takes place. To take one common example, under the Brussels Convention a person domiciled in a contracting state can be sued in the courts for the place where the harmful event occurred. But where does the harmful event occur, if for example a cookie transmits personal information about a person in the UK visiting a website hosted on a server in Luxembourg and operated by a company in Germany? A similar difficulty can arise in determining which system of law governs an issue. Under the Rome Convention, for example, the governing law of a consumer contract can depend on where the consumer's order was received. Where is that, if I use my laptop to place an order with a company in Italy using a server located in India? Problems can also arise in relation to many areas of substantive law - for example, in deciding whether our criminal law applies to online gambling, or to online pornography and fraud, or in applying our tax law, or our law of consumer protection. Conceivably, a transaction on the Internet might be regulated by the law of the country where the Internet user resides, or the law of the country where the website operator is based, or the law of the country where the server is located, to mention only some of the possibilities. If the location of an act that takes place "in cyberspace" is considered in a traditional way, the answer may be, "in several different jurisdictions at once", or it may be a location which has no significant connection with either party: say, where the critical event in a transaction between two parties in the UK takes place on a server located in Thailand.

In practice, one context in which this sort of issue has arisen is where a person makes information available over the Internet to the entire world. If that information offends against the law of a particular country, should the courts of that country assert jurisdiction over that person wherever he may happen to be located? In other words, should they assert a worldwide jurisdiction, at least in some cases?

In some legal contexts, there are well-established principles which can be applied in answering that question: for example, in order to establish the place of publication of defamatory material on a website, and the jurisdictional consequences of such publication. In that context, it has been held in a number of common law jurisdictions that defamatory material is published at the location where an Internet user obtains access to it on his or her computer, and jurisdiction can therefore be exercised on that basis.[3] In other contexts, different issues may arise.

An interesting example is a case which was brought in France against Yahoo! Inc, a US corporation, by groups campaigning against anti-Semitism.[4] At that time, Yahoo! operated an auction site similar to EBay via its yahoo.com portal, but not its yahoo.fr portal. The claimants complained that the auction site provided French residents with offers of Nazi memorabilia for sale, in breach of French law. The court rejected Yahoo!'s argument that the relevant act took place in the US, where the servers were located. It held that the accessibility of the auction site to French residents was sufficient to found jurisdiction in France and to make French law applicable. It rejected the argument that no order should be made by the French court, since it would be unenforceable in the US as a violation of the First Amendment guarantee of freedom of speech. It also rejected the argument that the nature of the Internet made it impossible to exclude French Internet users, on the basis that Yahoo! could identify IP addresses in France and filter them out. As you will know, websites can use geolocation

[3] See, for example, *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575.Jurisdiction may however be declined if the number of users accessing a site in the jurisdiction was minimal.
[4] *UEJF and Licra v Yahoo! Inc and Yahoo! France* (Tribunal de Grande Instance de Paris, 22 May 2000), available at www.lapres.net/yahen.

technology to tell where computers communicating with them are situated, and target them with advertising appropriate to their location. The auction site had indeed been greeting French users with French advertisements. It is true that identification can be avoided, or at least made more difficult, by the use of proxy servers and other devices, which are designed to enable an Internet user to conceal his true location, but few Internet users employ them. The court therefore ordered Yahoo! to take all appropriate measures to deter and prevent access to auctions of Nazi memorabilia on its site by French Internet users, or to pay a daily fine in default.

Yahoo! responded by ceasing to carry advertisements for Nazi memorabilia altogether, claiming that it was otherwise technically impossible to block French users. It also brought proceedings in the US against the French campaigners, seeking a declaration that the French court's order was unenforceable in the US as being in breach of the First Amendment. The district court granted Yahoo! the order it sought, but on appeal the Ninth Circuit dismissed Yahoo!'s case.[5] It emphasised that the French court's order did not require Yahoo! to restrict access to the auction site by Internet users based in the United States. One of the judges commented that Yahoo! was necessarily arguing that it had a First Amendment right to violate French criminal law and to facilitate the violation of French criminal law by others. The Supreme Court denied certiorari.[6] So Yahoo!'s challenge to enforcement failed; but the proceedings illustrate the point that the willingness of courts to accept jurisdiction over persons outside their borders does not mean that the judgments of those courts are necessarily easy to enforce in other jurisdictions.

A broadly similar approach to that of the French court was followed by a US court in a case concerned with intellectual property rights. A pornographic website based in Italy, operated by an Italian company known as Playmen, was held to be infringing the Playboy trademark in the US, since it

[5] United States Court of Appeals, Ninth Circuit. - 433 F.3d 1199, *Yahoo! Inc. v. LICRA and UEJF,* January 12, 2006.
[6] Order No 05-1302, 30 May 2006.

allowed and indeed solicited subscriptions by US residents, and then allowed them online access to its material. In doing so, it was held, it distributed infringing material in the US.[7] The court did not order the closure of the website. It accepted that a website owner could not be prohibited from operating its site merely because it was accessible from within a country in which its product was banned. But it found the accessibility of the material to subscribing customers in the US to be a breach of the trademark.

There are of course factual circumstances in which jurisdiction may not exist merely on the basis of the accessibility of a website, or in which courts will decline to exercise jurisdiction on *forum non conveniens* or other grounds. That can be seen, for example, in English defamation cases where jurisdiction was declined on the basis that, although the defamatory material was accessible online to users in the UK, hardly any had actually viewed it.[8] On a similar basis, some American courts have developed the interesting idea of a "sliding scale" approach to jurisdiction.[9]

What about the scope of remedial orders? The nature of the problem can be illustrated by the so-called right to be forgotten. The story begins in 2010 with Señor González, who complained to the Spanish Data Protection Agency that anyone who googled his name was provided with links to official announcements in a Spanish newspaper, dating from 12 years earlier, concerning the auction of his property as part of debt recovery proceedings. As he relied on the EU's 1995 Data Protection Directive,[10] the issue ended up before a Grand Chamber of the CJEU, and was decided last year.[11]

In relation to the facts of the case, it was found that Google Search was operated by Google Inc, a company based in the US. That company had subsidiaries in other countries, such as Google

[7] *Playboy Enterprises v Chuckleberry Publishing,* 939 F Supp 1032 (SDNY 1996).
[8] For example, *Jameel v Dow Jones & Co Inc* [2005] QB 946; *Al Amoudi v Brisard* [2007] 1 WLR 113.
[9] See, for example, *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).
[10] Directive 95/46.
[11] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (the directive AEPD)* C-131/12 (May 13, 2014).

Spain, based in Spain, which marketed and sold advertising services as its agent. Google Search was made available worldwide by Google Inc through the website google.com, and also through local versions such as, in Spain, google.es.

The CJEU held in the first place that the operator of a search engine, such as Google Inc, was a controller of the processing of personal data. As it had set up a subsidiary in a member state to sell the advertising space offered by the search engine, it followed that the processing of personal data which Google Inc controlled was carried out in the context of activities of an establishment of the controller on the territory of a member state. It therefore fell within the scope of the directive. On the merits of the complaint, the court said that the rights to privacy and to the protection of personal data, protected by the EU Charter of Fundamental Rights, "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name".[12] The court added that "that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question".[13] It followed that individuals should be able to apply to Google Inc to have links removed, and if it declined, could bring claims before a court or a data protection authority.

The "right to be forgotten" is highly controversial in the common law world, and the subsequent proposal for its inclusion in an EU regulation has attracted criticism from, amongst others, the House of Lords European Union Committee.[14] I don't propose to enter into that debate this evening. The judgment also raises many other questions, for example about its implementation, its relevance outside the EU, and whether the same approach should be adopted by other courts. The

[12] Para 97.
[13] Para 99.
[14] 2nd Report of Session 2014–15 (30 July 2014).

aspect of the case which particularly interests me for present purposes is the scope of the obligation to delist: an issue which can also arise in other contexts, such as defamation. Suppose that a court finds a violation of a national law related to a search engine. How should that finding be reflected in a remedy, given the global reach of the Internet? Should the operator be ordered to remove the objectionable links in all its versions of the search engine around the world, or only in the local version directed at the jurisdiction in question? The CJEU did not discuss this in its judgment.

In technical terms, Google could implement the right to delisting, where it exists, in three different ways. First, it could delist the objectionable links only from country-specific Google Search sites, such as google.es, while retaining the links at the root site for all of these national versions, namely google.com. This is the approach that Google in fact adopted in response to the CJEU ruling, and which, as far as I'm aware, it maintains to this day. After granting a delisting request, Google will remove the requested links across all European country-specific sites. European users almost always use their country-specific Google Search sites (in part because google.com automatically redirects them there, on the basis of an assessment of their location, using their IP address). But they can also access google.com, which still contains the links that were removed locally. As a result, it is possible, though uncommon, for European users to access search results that were delisted from the European Google Search sites.

Secondly, Google could use geolocation technology to prevent users in Europe from receiving the objectionable links as search results, regardless of which country-specific site they used. Geolocation technology was developed because it increases the effectiveness of Internet advertising, and it has become quite sophisticated. However, as I mentioned earlier, searchers can use anonymity preserving technologies, such as proxy servers, to conceal their geographical location. Whether search engines like Google possess the technical ability to geolocate users who attempt to conceal their location in that way is not clear. So, determined European users could, possibly, evade Google's geolocation filter to access search results that would otherwise be unavailable. In addition, the cost

trade-offs to companies of the use of geolocation filters, as compared with the domain-based approaches I shall discuss in a moment, are not clear.

Thirdly, Google could remove objectionable links from the main Google Search site, google.com. Links removed from google.com are also removed from all country-specific Google Search sites, and so removals from google.com affect search results in every country in the world. Technically, this may be the only perfect means of excluding access to the link by users from a specific jurisdiction. It is also said to be cheaper than using geolocation to filter out users from a particular country. So it is possible that, to conserve costs, search engine companies may choose to take information down globally rather than in a more tailored fashion. The point is illustrated by the Yahoo! case I discussed earlier, where the French court envisaged that Yahoo! would use geolocation technology to exclude French visitors from the .com site, but Yahoo! chose instead to delete the offending material altogether. One downside of this approach is its effect on freedom of expression: it may make economic sense for search engine operators to remove links worldwide to webpages which are arguably objectionable in a particular jurisdiction. The Yahoo! case was not of that kind on its facts, but it illustrates the point. The consequence is that, for commercial reasons, court orders may in practice have a greater chilling effect on freedom of expression than the court may have envisaged or intended.

The *Google Spain* case has prompted some commentators to suggest that the geolocation measures that the French court envisaged in the *Yahoo*! case are legally insufficient, at least where fundamental rights are concerned. Two responses come from different perspectives - that of regulators in Europe and that of an expert council convened by Google itself. In 2014, the European Commission's Article 29 Data Protection Working Party (whose members include representatives from each member state's supervisory authorities) issued guidelines, pursuant to its mandate to advise the EU on protecting individuals' personal data and on the free movement of data. The Working Party concluded that, to give full effect to data subjects' rights under the *Google Spain* ruling, delisting should

be effective on all relevant domains, including .com. The 2014 guidelines are not legally binding on search engines but are intended to guide European data protection authorities on how to assess complaints brought against search engines. For example, in June 2015, France's data protection regulator relied on these guidelines and ordered Google to apply delinking to google.com or be subjected to financial sanctions.

Google itself convened a group of independent experts, who concluded that the competing interests on the part of users, especially those outside Europe, in being able to access information in accordance with the laws of their own country supported Google's current approach.[15] Google's experts also expressed concern about the global precedent that could be set by efforts to suppress links from search engines on a universal basis.

Unsurprisingly, the Commission's proposed General Data Protection Regulation, intended to replace the Data Protection Directive, follows the approach of the Article 29 Working Party.

In the long run, international law might be thought to offer the ideal means of resolving the issues I have discussed. There are of course some important international agreements, such the 2004 Convention on Cybercrime, and other international documents promulgated by UN agencies. At the regional level, there are a number of EU regulations and directives dealing with specific issues, such as the Directive on Electronic Commerce, concerned with the liabilities of ISPs and other intermediaries,[16] as well as a number of judgments of the CJEU besides the *Google Spain* case.[17] There are also a number of Council of Europe instruments, as well as some important judgments of the European Court of

[15] The full report is available at www.cil.cnrs.fr/CIL/IMG/pdf/droit_oubli_google.pdf.
[16] Directive 2000/31/EC, implemented by the Electronic Commerce (EC Directive) Regulations 2002. Similar laws exist in other jurisdictions, such as the US: see the Communications Decency Act 1996, s 230, considered in such cases as *Barnes v Yahoo! Inc* 570 F.3d 1096 (9th Circuit. 2009) and *Klayman v Zuckerberg* (US Court of Appeals for the District of Columbia Circuit, 13 June 2014).
[17] Examples include Joined Cases C-236/08 to C-238/08 *Google France and Google,* 23 March 2010; Case C-324/09 *L'Oréal and Others,* 12 July 2011; Case C-70/10 *Scarlet Extended,* 24 November 2011; Case C-360/10 *SABAM,* 16 February 2012; and Case C-291/13 *Papasavvas,* 11 September 2014.

Human Rights.[18] But most legal questions relating to the Internet will continue to be governed by national law for the foreseeable future.

In that context, given the various remedial options available, how should judges decide the scope of the remedies they award, to the extent that their hands are not tied by domestic legislation or EU law? Should courts make orders which will be watertight in respect of all users in their jurisdiction, even if the result is collaterally to affect all users around the world, or can a more qualified level of effectiveness be accepted? Should the answer depend on the court's assessment of the nature of the harm, and the relationship between the particular harm and the court's authority? What weight ought to be given to constitutional claims about rights to have information disseminated, as well as rights not to? What role do concerns about comity play – comity towards other jurisdictions' laws and constitutional principles, and towards other courts - when rulings relate to the Internet? If Europe seeks to apply its data protection law universally, should other jurisdictions also seek to apply universally their own laws, for example prohibiting certain political, religious or sexual speech or, conversely, insisting on access to information universally for all online users?

These questions are particularly acute where the jurisdictions involved have widely differing cultures in relation to the subject-matter in question. In the *Yahoo!* case, for example, the French court emphasised that France was profoundly wounded by the atrocities committed during the Second World War against its Jewish citizens. Many continental European countries attach great importance to the privacy and dignity of the individual, all the more so when the unpleasant things said about him happen to be true. As *Google Spain* and the more recent case of *Schrems*[19] illustrate, the CJEU sees the protection of personal data as a fundamental right. On the other hand, the US attaches particular importance to freedom of speech, and has a highly developed culture of freedom of information. There, the protection of personal data is considered mainly in terms of consumer protection. Other countries,

[18] An example is *Defi AS v Estonia* [2015] EMLR 563, concerned with liability for unlawful comments posted on its news portal.
[19] *Schrems v Data Protection Commissioner* (Case C-362/14), 6 October 2015.

such as Iran and Saudi Arabia, may have different priorities again. Should these differences of culture be taken into account? How are conflicting rulings to be avoided? How do courts monitor and enforce compliance with their orders across borders?

There is a valuable discussion of some of these issues in a recent judgment of the Court of Appeal of British Columbia. In the case of *Equusteck Solutions Inc v Google Inc*[20] the plaintiffs were manufacturers. The defendants, who were their former distributors, sold similar products over the Internet, allegedly in breach of the plaintiffs' intellectual property rights and in breach of confidence. The court had made orders against the defendants at a time when they operated in Canada. They then moved their operations elsewhere, offering their products through websites which they controlled, located around the world. In order to attract customers, they relied on search engines to direct members of the public making enquiries about the relevant kinds of product to their websites. The majority of their customers were not Canadian. The plaintiffs responded by seeking an injunction against Google Inc, to force it to remove the defendants' websites from its search results. Google Inc is a US company, without any presence or any servers in British Columbia. But the court held that it had jurisdiction under the relevant law, because Google Inc did business in the Province: it sold advertising space there, and it obtained data there using its crawler software, Googlebot, which compiles the index on which the search engine is based.

The question then was what should be the scope of any remedy granted. Google raised the spectre of its being subjected to restrictive orders from courts in all parts of the world, each concerned to enforce its own domestic law. The court was unmoved. "It is the world-wide nature of Google's business and not any defect in the law that gives rise to that possibility", the court said. It added that the threat of multi-jurisdictional control was over-stated. Courts considered many matters other than

[20] 2015 BCCA 265 (June 11, 2015).

territorial competence and the existence of jurisdiction over the parties: "courts must", it said, "exercise considerable restraint in granting remedies that have international ramifications".

Google then argued that the Canadian court was not competent to regulate the activities of non-residents in foreign jurisdictions. That proposition was rejected: the courts had been issuing orders affecting non-residents' activities in other jurisdictions for many years. An example given was the *Mareva* injunction. The court accepted, however, that the extent to which it would issue worldwide orders was affected by pragmatic considerations and by comity. The only comity concern raised by Google was that the proposed order could interfere with freedom of expression in other countries. The court accepted that the importance of freedom of expression should not be underestimated. It said that courts should be very cautious in making orders that might place limits on freedom of expression in another country. Where there was a realistic possibility that an order with extraterritorial effect might offend another state's core values, the order should not be made. But in the case before the court, there was no realistic assertion that to prohibit the defendants from advertising products that violated the plaintiffs' intellectual property rights would offend the core values of any nation. It seems to me that that must be right: preventing the breach of intellectual property rights can be taken to be a universal principle of trade law.

There seems to me to be great deal of good sense in this judgment, if I may respectfully say so. I would not be surprised to find it cited in our courts.

Drawing these thoughts together, many questions arise from the cases I have discussed. Of course, in areas where matters are dealt with by legislation, the courts will apply the legislation, and in areas where there is no legislation, the courts can generally be expected to apply existing principles, as they have done in areas such as defamation, with such adaptations as may be necessary. But, as I sought to explain in the earlier part of my talk, a number of issues arise from the fact that the communication

of data by means of the Internet is difficult to contain territorially, and that many of the operators carry out their activities on a worldwide basis. The publication of information on a website operated in the US may, for example, expose the publisher to civil or criminal liability in any country of the world, on the basis of the law of those countries. And it might be said, as in effect the Canadian court said, that he can hardly complain, if it is his choice to make the information available on a worldwide basis. At the same time, court orders with an extraterritorial effect, whether made by the courts of this country or by courts overseas, may run up against the problem that different constitutional orders attach different weights to such matters as privacy, free expression and free speech. Court orders made in one jurisdiction may not be enforced in another jurisdiction if, for example, they offend against constitutional rights or public policy. So a technology, and a way of doing business, which crosses borders inevitably raises issues concerning the interaction of the jurisdictions of national or supranational courts, the remedies they can or should grant, and the enforcement of those remedies.

These issues will inevitably come time and again before the courts in this country and elsewhere. Developing a workable approach to them is going to be one of the major legal challenges of our times.