# 1

# The Regulated End of Internet Law, and the Return to Computer and Information Law?

*Christopher T. Marsden**

This chapter is both a retrospective, and also even a requiem, for the 'unregulation' argument in Internet law in the past twenty-five years, and a prospective on the next twenty-five years of computer (or cyber) law,[1] in which many of the expert treatises of the 1990s need to be dusted down and reabsorbed.[2]

The global communications network connected by the Internet Protocol has transformed the consumer/prosumer and small business experience of electronic communication.[3] The Internet is not a lawless, special unregulated zone; it never was.[4] Now that broadband Internet is ubiquitous, mobile, and relatively reliable in urban and suburban areas, it is being regulated as all mass media before it. The major gatekeepers are regulated for the public good and public interest, whether that be access providers through infrastructure sharing, electronic privacy, cybersecurity and network

* I wish to thank the contributors to this edited collection and its editor, the panelists and participants at the Wharton School symposium "After the Digital Tornado" on 10 November 2017, and participants at the Georgetown Technology Law Review symposium on 23 February 2018 on "Platform Law," especially Julie Cohen and Mireille Hildebrandt. I also wish to thank the contributors and participants at the Münster Institute for Information and Telecommunications Law twentieth anniversary symposium in Berlin, Germany on 15 July 2017, especially Bernd Holznagel, and the contributors and participants at the eleventh annual Gikii symposium in Winchester, England, on 15 September 2017, especially Lilian Edwards, Andres Guadamuz, Paul Bernal, Daithi MacSithigh, and Judith Rauhofer. All errors and omissions remain my own.

[1] Eastham, Laurence (2011) *Interview with SCL's New President, Richard Susskind*, Society for Computers and Law, 23 August, at www.scl.org/articles/2191-interview-with-scl-s-new-president-richard-susskind. See also Susskind, Richard (2018) *Sir Henry Brooke – A Tribute*, Society for Computers and Law, at www.scl.org/articles/10221-sir-henry-brooke-a-tribute.

[2] A good introduction is Reed, Chris (2010) *Making Laws for Cyberspace*, Oxford: Oxford University Press, especially at pp. 29–47.

[3] See generally for European law, Edwards, Lilian (ed., 2018) *Law, Policy, and the Internet*, Oxford: Hart Publishing; for US law, Goldman, Eric (2018) *Internet Law Cases and Materials*. For an annotated bibliography of classic academic legal writing, see Marsden, Chris (2012) *Internet Law*, Oxford Bibliographies Online, New York: Oxford University Press.

[4] For early UK cases, see Athanasekou, P. E. (1998) Internet and Copyright: An Introduction to Caching, Linking and Framing, *Journal of Information, Law and Technology* (JILT); Opinion of Lord Hamilton in *The Shetland Times Ltd* v. *Dr Jonathan Wills and Zetnews Ltd*. Court of Session, Edinburgh 24 October 1996, at www.linksandlaw.com/decisions-87.htm.

neutrality regulation, or the social media, e-commerce and search giants through various duties of care including those for notice and rapid action – in many cases, requiring takedown of allegedly illegal material in a day or even an hour,[5] and notification of breach of security and privacy to the customer.[6] An Internet law expert arriving in a time machine from the mid-1990s would find all this quite shocking.

We have now come full circle from computer law prior to the Internet's explaining the importance of robotics, cybernetics, and Electronic Data Interchange (EDI) in the 1980s; to an explanation of the Internet's impact on the law in the 1990s that ranged across the entire syllabus including constitutional law and jurisprudence;[7] to more specialist examinations of law in such areas as intellectual property and telecommunications in the 2000s; to a realization that the future was delayed not denied and that cyberlaw is vital to understanding regulation of platforms, of artificial intelligence and robotics, of blockchains, of automated vehicles, and of disinformation in our democracies.

The 2020s will finally be the decade of cyberlaw, not as 'law of the horse', but as digital natives finally help bring the law syllabus, legal practice, and even legislatures into the Information Society.

In the first part of the chapter, I explain how the cyberlawyers of the 1990s dealt with regulation of the then novel features of the public Internet. Internet law was a subject of much interest in the 1990s in the US, and some specialist interest in UK and Europe.

In Part 2, I explain the foundational rules for the adaptation of liability online initially focused on absolving intermediaries of legal responsibility for end user-posted content. This exceptionalist approach gradually gave way. While some US authors are hamstrung by a faith in the myth of the superuser and somewhat benign intentions of corporations as opposed to federal and state government, there has been a gradual convergence on the role of regulated self-regulation (or co-regulation)[8] on both sides of the Atlantic.[9]

In Part 3, I argue that the use of co-regulation has been fundamentally embedded since European nations began to enforce these rules, with limited enforcement in

[5] European Commission (2017) Communication on Tackling Illegal Content Online: Towards an Enhanced Responsibility of Online Platforms; European Commission (2018) Recommendation on Measures to Effectively Tackle Illegal Content Online, published 1 March.

[6] Belli, Luca and Zingales, Nicolo (eds. 2017) *Platform Regulations: How Platforms Are Regulated and How They Regulate Us*, FGV Direito Rio, Brazil, at https://bibliotecadigital.fgv.br/dspace/handle/10438/19402.

[7] An excellent review is provided by chapters 1–3 in Murray, Andrew and Reed, Chris (2018) *Rethinking the Jurisprudence of Cyberspace*, Cheltenham: Edward Elgar.

[8] Holznagel, Bernd and Hartmann, Sarah (2017) Do Androids Forget European Sheep? – The CJEU's Concept of a 'Right to Be Forgotten' and the German Perspective, in Russel Miller (ed.) *Privacy and Power – A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge: Cambridge University Press, pp. 586–614.

[9] See, for instance, Frischmann, Brett, M. (2005) An Economic Theory of Infrastructure and Commons Management, Minnesota Law Review, Vol. 89, 917–1030, at https://ssrn.com/abstract=588424, discussed in Marsden, Chris (2017) *Network Neutrality: From Policy to Law to Regulation*, Manchester: Manchester University Press.

which judges and regulators stated that business models largely focused on encouraging illegal posting would not be protected. Settled policy on liability, privacy, trust, encryption, open Internet policies against filtering, were arrived at as a result of expert testimony and exhaustive hearings.

Finally, in Part 4, I argue that hanging those policies on a whim results in potentially catastrophic results in terms of untying the Gordian knots of intermediary safe harbour, privacy, copyright enforcement, and open Internet European regulations.

It is often forgotten that the Werbach's 'Digital Tornado' paper[10] heralded a model of limited state regulation, but very substantial responsible collective self-regulation ('consensus and running code') within transnational law.[11] When that pact was broken by 4Chan script kiddies and two billion Facebook users, it moved regulation away from the responsible collectivism of the pioneers' Internet.

There were three views of regulation in 1997: the type of self-regulation I have described; a belief in state regulation by those existing vested interests in broadcast, telecommunications and newspapers; and a third view that state regulation was inevitable as the Internet became ubiquitous but needed to be as reflexive and responsive as could be maintained with human rights responsibilities.

The perspective of today allows us to rethink the apparent triumph of the first view. If 2018 can in retrospect be seen as the year that the 'Tech Bros' view of regulation faltered and was replaced (to some extent) by state and supranational intervention, then the third option, of what I describe as co-regulation, appears to be supplanting that self-regulation option.[12] The state intervention was most notable in both scale and scope in European Union law, for data protection, consumer/prosumer protection, and also for competition enforcement.

## PART 1: 1990S' HISTORY OF INTERNET LAW

The Internet was developed in the 1960s at a group of research institutes in the United States and the United Kingdom.[13] The Internet is a network of approximately 50,000

[10] Werbach, Kevin (1997) Digital Tornado: The Internet and Telecommunications Policy, Federal Communications Commission Office of Plans and Policies Working Paper 29. Washington, FCC.

[11] See most recently, Mahler, Tobias (2019) *Generic Top-Level Domains: A Study of Transnational Private Regulation* (Elgar Studies in Law and Regulation) Cheltenham: Edward Elgar. See also Marsden, Chris (forthcoming) Transnational Information Law, in Peer Zumbansen (ed.) *Oxford Handbook of Transnational Law*, Oxford: Oxford University Press.

[12] For co-regulation, see Senden, Linda A. J. (2005) Soft Law, Self-regulation and Co-regulation in European Law: Where do they Meet?, *Electronic Journal of Comparative Law*, Vol. 9, No. 1, January 2005, at https://ssrn.com/abstract=943063; Marsden, Chris (2011) *Internet Co-Regulation*, Cambridge: Cambridge University Press. Historically, see the Max Planck Institute study: Collin, Peter (2016) Justice without the State within the State: Judicial Self-Regulation in the Past and Present, *Moderne Regulierungsregime*, Vol. 5, IX, 373.

[13] Clark, David D., Field, Frank, and Richards, Matt (2010) *Computer Networks and the Internet: A Brief History of Predicting Their Future*, CSAIL Working Paper, at http://groups.csail.mit.edu/ana/People/DDC/Working%20Papers.html; first international links were from the United States to Norway, see

autonomous systems, which are interconnected by the Internet Protocol. The Internet became an information network of critical mass in the 1990s with the rise of Bulletin Board Services (BBS),[14] still more so with the growth of commercial Internet service providers (ISPs) in the late 1980s, and eventually a mass market artefact with the development of the World Wide Web ('WWW') and release of commercial web browsers in 1993–1994. The Internet developed as a self-regulated academic network,[15] and its emergence as a commercial platform that would rapidly permeate through society was largely unpredicted.[16] Kahin and Nesson explained that the development of the Internet was bottom up and self-regulatory, and explored the emerging tensions as other nation-states began to assert a regulatory role.[17]

Internet growth, together with its increasing commercial exploitation, was accompanied by an explosive growth in United States' scholarship. In 1993, Reidenberg explained that information had become an international commodity, ill served by existing legal frameworks poorly adapted due to their focus on the tangible aspects of information-intensive products and insufficient attention to the intangible aspects of information content.[18] Reidenberg extended the argument that technology can create an environment in the absence of legal rules in his ground-breaking conception of *lex informatica*. In the absence of *ex ante* sovereign power and legal rules, technology can symbiotically create de facto commercial regulation in much the same way as the mediaeval *lex mercatoria*.[19] He extensively spelled out the use of technology as a parallel form of regulation.

Building on Reidenberg's insights, Johnson and Post made the classic argument for the Internet as a borderless self-regulatory medium that should be permitted to develop with less of the state-imposed restrictions that impeded the growth and development of earlier media.[20] The growth of the application of law to its

Brown, Ian (ed., 2012) *Research Handbook on Governance of the Internet*, Cheltenham: Edward Elgar, chapter 1.

[14] Goldman, Eric S. (1994) Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions, *Hastings Comm/Ent Law Journal*, Vol. 16, 87.

[15] Clark, David D. and Blumenthal, Marjory S. (2011) The End-to-End Argument and Application Design: The Role of Trust, *Federal Communications Law Journal*, Vol. 16, 357–70.

[16] De Sola Pool, Ithiel (1983) *Technologies of Freedom*, Harvard: Harvard University Press. Pool analyzed the confrontation between the regulators of the new communications technology and the First Amendment, presciently forecasting the legal conflict that the Internet created between freedom of expression and government control/censorship. See also Kahin, Brian and Keller, James H. (eds., 1997) *Coordinating the Internet*, Cambridge, MA: MIT Press.

[17] Kahin, Brian and Nesson, Charles (eds., 1997) *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, Cambridge, MA: MIT Press.

[18] Reidenberg, Joel (1993) Rules of the Road for Global Electronic Highways: Merging the Trade & Technical Paradigms, *Harvard Journal of Law and Technology*, Vol. 6, 287, at http://jolt.law.harvard.edu/articles/pdf/v06/06HarvJLTech287.pdf.

[19] Reidenberg, Joel (1998) Lex Informatica: The Formulation of Information Policy Rules through Technology, *Texas Law Review*, Vol. 76, 553–93.

[20] Johnson, D. and Post, D. (1996) Law and Borders: The Rise of Law in Cyberspace, *Stanford Law Review*, Vol. 48, 1367–75.

emergence was also unpredictable, although Johnson and Post argued for an 'exceptionalism' to permit this globalized unregulated medium to grow unfettered by state censorship, which they saw as both normatively and substantively unjustified. They drew on United States' constitutional law and history in the argument. They suggest a structured, principled, and internationally acceptable manner for national legislators to respond to the Internet. Lessig, while rejecting excessive state intervention, warned that self-regulation could lead to an Internet controlled by corporate interests.[21] Lessig argued that state forbearance was rapidly resulting in private regulation by new monopolies, to supplement the existing regulation by technical protocols.

Although cyber-exceptionalism became the dominant viewpoint among scholars, it was not without its opponents. Goldsmith made a legal positivist stand against the Post-Johnson Internet exceptionalism, seeing as both normatively and substantively flawed any 'claim that cyberspace is so different from other communication media that it will, or should, resist all governmental regulation'.[22] He asserted that it can be regulated, including via conflict of laws rules, although this is not a normative position on whether law should utilize its tools to regulate the Internet. In an early trans-Atlanticist article arguing against Internet exceptionalism and reactive national Internet regulation, Mayer-Schönberger and Foster argued that the global information infrastructure limits both absolutists and regulators.[23] The emerging internationalization of the Internet would lead to both jurisdictional conflicts as well as a clash of rights principles, as foreseen by Mayer-Schönberger and Foster. Samuelson argued persuasively that legislators must ensure that the impending rule making for the Internet is proportional in both economic and human rights terms to the needs and demands of users, as well as coordinated internationally.[24] Samuelson accepted the rise of the state, the need for sovereign intervention, and the efficiency self-regulation had provided, in arguing for principles for legislating on the Internet.

There have been extensive discussions as to the provenance of a field termed 'Internet' or 'cyber' law since the mid-1990s. As the law was colonizing the metaphorical "cyberspace" – communications between computer users over the Internet – most of the most authoritative and pioneering legal scholarship with regard to the new medium dates to the 1990s. Several offline subjects have themselves incorporated large literatures from their digital form, including intellectual property, non-networked computer law, telecommunications, privacy, cybercrime,

[21] Lessig, Lawrence (2006) *Code and Other Laws of Cyberspace*, New York: Basic Books. Revised 2nd ed. titled *Code v2.0*, at http://codev2.cc/.

[22] Goldsmith, Jack L. (1998) Against Cyberanarchy, *University of Chicago Law Review*, Vol. 65, 1199.

[23] Mayer-Schönberger, Viktor and Foster,Teree E. (1997) A Regulatory Web: Free Speech and the Global Information Infrastructure, *Michigan Telecommunications and Technology Law Review*, Vol. 3, 45, at www.mttlr.org/volthree/foster.pdf.

[24] Samuelson, P. (2000) Five Challenges for Regulating the Global Information Society, in Chris, Marsden (ed.) *Regulating the Global Information Society*, Routledge: London.

and media content regulation. As the Internet was 'born global' but first became widely deployed in the United States, much of the literature has a bias in that direction.

Many argue that the effects of digital information retrieval on the law applies across all areas with some relevance, especially for intellectual property, and that Internet law should be considered part of the law of contracts, competition, the Constitution, and so on, with narrow exceptions for such issues as legal informatics, and telecommunications law, which are being transformed by technology, and therefore cannot remain distinct[25]. Easterbrook famously argued along these lines that there is no field of 'Internet law', any more than there is the 'law of the horse'.[26] Lessig responded that the transformative effects of the Internet on law, in areas including free expression, privacy, and intellectual property, are such that it offers lawyers a radically new route to thinking about private regulation and globalization, the limits of state action, as well as a powerful metaphor for explaining these wider changes to law students.[27] Sommer dismissed Lessig's claims regarding the exceptionalism of cyberlaw, arguing that 'a lust to define the law of the future' is dangerous, and can create bad taxonomy and bad legal analysis.[28]

Academics have constantly argued that the lack of general academic expertise and the emergence of the field mean that Internet law is a necessary short-term distinct study area, which may eventually be reintegrated into its constituent parts, as an inevitable eventual assimilation. Kerr explained two divergent views of Internet law. The first is an internalized expert view of the law, the second a technophobic view. Kerr concluded that two perspectives will converge and evolve, as more people understand the underlying technologies involved, and the useful middle ground.[29] In a survey essay into the origins of the Internet law debate, Guadamuz argued that several new fields are emerging from the study of computers and law, including legal informatics, artificial intelligence (AI) and law, and that Internet law can provide new insights into established fields that provide contemporary context for the theoretical study of several subjects, and the profession's development as a whole.[30] Guadamuz argued that the 'Attack of the Killer Acronym' was preventing accessibility to Internet law for the wider legal profession, clients (and faculty).

[25] Marsden, C. (2010) *Network Neutrality: Towards a Co-Regulatory Solution*, London: Bloomsbury, at 216–19.

[26] Easterbrook, Frank H. (1996) *Cyberspace and the Law of the Horse*, Chicago: University of Chicago Legal Forum, 207.

[27] Lessig, Lawrence (1999) The Law of the Horse: What Cyberlaw Might Teach, *Harvard Law Review*, Vol. 113, 501.

[28] Sommer, Joseph H. (2000) Against Cyberlaw, *Berkeley Technology Law Journal*, Vol. 15, 3, at www.law.berkeley.edu/journals/btlj/articles/vol15/sommer/sommer.html.

[29] Kerr, Orin S. (2003) The Problem of Perspective in Internet Law, *Georgetown Law Journal*, Vol. 91, 357, at http://ssrn.com/abstract=310020.

[30] Guadamuz, Andrés (2004) Attack of the Killer Acronyms: The Future of IT Law, *International Review of Law, Computers & Technology*, Vol. 18, No. 3, 411–24.

Larouche later argued that the object of information law has mutated, scope for public intervention has been rolled back, implementation of any form of public intervention has been made more difficult, and that information law has seen its main topics expropriated by more traditional topics. The law syllabus is being digitized, literally (e-books, e-syllabi, e-libraries). He predicted the end of Internet law as a subject and the abstraction of information law to move away from a specific technology (except telecoms, media law). As a result, he argued that a 'future information law' will be radically amended.[31] Goldman argued for an Internet law that can be taught using new pedagogical elements employed on a survey-type course, and argued against Easterbrook that the volume of Internet-specific legislation and case law means that common law cannot provide a sufficient grounding for students to understand the transformations wrought by Internet law.[32]

Specialization happened to some extent, with e-commerce part of standard contract law, platform dominance in competition law, digital copyright (and patent) law, cybercrime in criminal law, and so on, as Murray described.[33] Some of the more interesting specialist Internet law academic literature from the 1990s (and early 2000s) has also stood the test of time,[34] for instance, on network effects,[35] cyberlaw, and control by code or *lex informatica*,[36] free and open source software and control of the online environment,[37] network neutrality and the regulation of intermediaries by their networked environment,[38] and the creation of monopoly gatekeepers resisting yet also predicting the dominance of Google, Amazon, Facebook, Apple, and Microsoft (GAFAM).[39] Internet law has been approached as a private and public law, with policy perspectives from law and economics as well as sociolegal studies. The overviews that best introduce the topic to general readers contain contributions that provide both a commercial and a public law perspective. Some important

[31] Larouche, Pierre (2008) On the Future of Information Law as a Specific Field of Law, TILEC Discussion Paper No. 2008-020, at http://ssrn.com/abstract=1140162.

[32] Goldman, Eric (2008) Teaching Cyberlaw, Santa Clara University School of Law Legal Studies Research Papers Series Working Paper No. 08-57, at http://ssrn.com/abstract=1159903.

[33] Murray, A. (2013) Looking Back at the Law of the Horse: Why Cyberlaw and the Rule of Law are Important, *SCRIPTed*, Vol. 10, No. 3, 310, at http://script-ed.org/?p=1157.

[34] See, for instance, Marsden, Chris (2012) *Oxford Bibliography of Internet Law*, New York: Oxford University Press.

[35] Lemley, Mark and McGowan, David (1998) Legal Implications of Network Economic Effects, *California Law Review*, Vol. 86, 479, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=32212.

[36] Lessig, Lawrence (1999) *Code and Other Laws of Cyberspace*, New York: Basic Books.

[37] Benkler, Yochai (2002) Coase's Penguin, or Linux and the Nature of the Firm, *Yale Law Journal*, Vol. 112, 369, at www.benkler.org/CoasesPenguin.html.

[38] Wu, Tim (2003) When Code Isn't Law, *Virginia Law Review*, Vol. 89, 679, at papers.ssrn.com/sol3/papers.cfm?abstract_id=413201.

[39] Zittrain, Jonathan (2006) The Generative Internet, *Harvard Law Review*, Vol. 119, 1974, at papers.ssrn.com/sol3/papers.cfm?abstract_id=847124.

contributions have focused on US law and policy,[40] and relatively few works provide a trans-Atlantic context.[41]

The world has changed less than we think it has in the last generation, and the battle between tyranny and freedom is eternal and geographical.[42] Both the twenty-first-century Internet and the nineteenth-century telegraph are controlled by the Five Eyes (the Anglo-American powers and their former colonies in Singapore and Oceania). While the reach of international human rights law was severely limited in the nineteenth century, largely a matter of humanitarian aspects of the law of war and the extraterritorial application of domestic anti-slavery laws by the hyper-power Great Britain, we now live in what are claimed to be more enlightened times. The cabling of the planet for the Internet uses much the same undersea telegraph lanes and developments from those technologies. The first Internet link outside North America was to Norway (as part of the North Atlantic Treaty Alliance) in 1973. We have wired Africa and have an interplanetary Internet. Geography matters, and so does territorial sovereignty. Information flows through those cables, and whoever controls the cables controls the information. The tapping of telegraph lines and blocking of encrypted messages was de rigueur in the Victorian era but this policy has been challenged under international human rights law in the twenty-first century.

The likelihood that multistakeholder civil society is able to exercise useful scrutiny and control over hyper-power politicians and their obedient corporate clients or partners may appear remote, and the call for international norms for human rights law quixotic. It could mark what some might call a tectonic shift in governance of communications. Cables may girdle the Earth in only 66.8 light milliseconds, but we continue to observe covert Internet surveillance in the shadowy half-light of governance of the corporations and surveillance agencies that have for so long controlled our information.[43]

## PART 2: A VERY SHORT INTERNET LIABILITY LEGISLATIVE HISTORY

These foundational rules for the adaptation of liability online focused on absolving faultless (and low fault, the line is shifting) intermediaries of liability for end user-posted

[40] Lemley, Mark, Menell, Peter S., Merges, Robert P., and Samuelson, Pamela (2011) *Software and Internet Law*, Gaithersburg, MD: Aspen Law & Business, 4th ed.; Thierer, Adam (ed., 2003) *Who Rules the Net? Internet Governance and Jurisdiction*, Washington, DC: Cato Institute.

[41] Yaman, Akdeniz, Walker, Clive, and Wall, David (eds., 2001) *The Internet, Law and Society*, London: Longman; Edwards, Lilian and Waelde, Charlott (eds., 2009) *Law and the Internet*, 3rd ed., Oxford: Hart Publishing; Marsden, Chris (ed., 2000) *Regulating the Global Information Society*, London: Routledge; Hedley, S. (2006) *The Law of Electronic Commerce and the Internet in the UK and Ireland*, London: Routledge-Cavendish.

[42] Marsden, Chris (2004) Hyperglobalized Individuals: the Internet, Globalization, Freedom and Terrorism, *Foresight*, Vol. 6, No. 3, 128–40.

[43] Marsden, Chris (2014) Hyper-Power and Private Monopoly: the Unholy Marriage of (Neo) Corporatism and the Imperial Surveillance State, *Critical Studies in Media Communication*, Vol. 31, No. 2, 100–108, at www.tandfonline.com/doi/full/10.1080/15295036.2014.913805.

content. More than two decades after *ACLU* v. *Reno* and the 'Information Superhighway' metaphor of Al Gore and Bill Clinton's first term is as useful a time as any to look back to the future. Settled policies were arrived at as a result of expert testimony and exhaustive hearings, on liability, privacy, trust, encryption, open Internet policies against filtering. Changing those policies now may result in potentially catastrophic untying of the Gordian knots of intermediary safe harbour, privacy, copyright enforcement, and open Internet European regulations.

The legislation that underpins intermediary liability was introduced in an extraordinary 'dot-com' boom in the period 1996–1999, frequently dated to start on 12 April 1996, when Yahoo! underwent an initial public offering, shares making 270 per cent profit for investors on a single day. The growth of Yahoo! reflects the heady valuations of Internet stocks in the period with its peak at $118.75 a share on 3 January 2000 crashing to $8.11 on 26 September 2001 – lower than the price of its IPO.[44] The rise and fall of broader telecoms stocks (the Internet's infrastructure plumbing) of about forty-two months was documented by Malik as amounting to an excessive valuation of about $750 billion.[45] A regulatory outcome of the large-scale fraud, accounting irregularity, and generalized lack of regulation in that period is the lack of proper investigation to learn the lessons of that boom and bust beyond the Sarbanes-Oxley Act 2002.[46] This may have contributed in small part to the failure of regulation, and far greater losses, of the 'Great Recession' of 2008–2009 and the 'Age of Austerity' that followed.[47]

Two myths need rebutting to understand the 'self-regulatory settlement' of Internet law. The first is that the United States settled on self-regulation and a hands-off approach. While this was the spirit of the Digital Tornado paper, it was very much unreflective of the 104th Congress that voted through the *Communications Decency Act* as part of the *Telecommunications Act 1996*.[48] In the US, liability regimes have differed according to speech-based and copyright-based liabilities. *Communications Decency Act* 1996 s.230 provides that 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content

[44] Odlyzko, Andrew (2003) *Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation*, December 29, at www.dtc.umn.edu/»odlyzko. For Yahoo! rise and fall, see https://en.wikipedia.org/wiki/Yahoo!#Expansion.

[45] See, generally, Malik, Om (2003) *Broadbandits: Inside the $750 Billion Telecom Heist*, Wiley & Sons.

[46] Pub. Law No. 107-204, 15 U.S.C. §§ 7201 et seq. (2003).

[47] Wren-Lewis, Simon (2015) The Austerity Con, *London Review of Books*, Vol. 37, No. 4, 9–11. UK neoliberal austerity lasted until 2018, in contrast to the US under President Obama's stimulus programme from 2010. For a US perspective, see Paul Krugman (2015) The Austerity Delusion, *The Guardian*, 29 April, at www.theguardian.com/business/ng-interactive/2015/apr/29/the-austerity-delusion; Romano, Roberta (2004) *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, New York University Law and Economics Working Paper 3, at http://lsr.nellco.org/nyu_lewp/3.

[48] 47 U.S.C. § 230. See Cannon, Robert (1996) The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway, *Federal Communications Law Journal*, Vol. 51, 74.

provider.'[49] This language might shield ISPs from liability for subscriber copyright infringement as well. However, Section 230(e)(2) specifically states: 'Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.' Section 230 established the concept of limited liability.[50] The *Digital Millennium Copyright Act 1998* s.512 laid out detailed rules for copyright infringement and the action required of intermediaries when notice of infringement, as paid out in DMCA, was sent. The introduction on 30 June 1995 of the *Internet Freedom and Family Empowerment Act* to amend the omnibus *Telecommunications Act of 1934*, was designed in part to mandate filters against adult pornography in all United States' households, and the eventual law as amended was voted through 420–4 on 4 August 1995,[51] remaining the federal law until part struck down in the famous *ACLU* v. *Reno* Supreme Court case on 26 June 1997.[52]

This non-filtered Internet regime, which arrived by accident as a result of constitutional convention, has been developed over time, and maintains a significant degree of difference from the gradually less permissive intermediary regime now permitted in the European Union.[53] Note that the 105th and 106th Congress were largely obsessed with attempting to impeach President Clinton for perjury, related to a sexual misconduct that was first publicized via that unrestricted Internet that Congress had attempted to control in 1995–7.[54] Attempts to reform the law in the period 2000 onwards were partially successful in restricting government-funded Internet services in for instance libraries, e.g. *Children's Internet Protection Act 2001*,[55] although statutes such as *Child Online Protection Act 1998* were struck down by the Supreme Court.[56]

There is thus a patchy history of US federal legislators attempting to restrict Internet harms and place restrictions on Internet access, struck down by the Supreme Court defending individual liberty against censorship.[57] In the absence of an active Supreme Court, Europe's lawmakers have faced fewer restrictions on controlling the Internet, although the liability regime is only modestly different. As Holznagel indicates, US courts have applied 'safe harbour' provisions to widely

[49] 47 U.S.C. § 230(c)(1).

[50] The Communications Decency Act was Part V of the Telecommunications Act of 1996, in which S.222 deals with privacy and transparency.

[51] On the roll call vote, see www.congress.gov/amendment/104th-congress/house-amendment/744.

[52] *ACLU* v. *Reno*, 521 U.S. 844, overturned s.223. Rappaport, Kim L. (1997) In the Wake of *Reno* v. *ACLU*: The Continued Struggle in Western Constitutional Democracies with Internet Censorship and Freedom of Speech Online, *American University International Law Review*, Vol. 13. 765.

[53] Guadamuz, Andres (2018) Chapter 1: Internet Regulation, inLilian Edwards (ed.) *Law, Policy and the Internet*, Oxford:Hart/Bloomsbury Publishing.

[54] DrudgeReport Archives (1998), *Newsweek Kills Story On White House Intern*, 17 January, at www.drudgereportarchives.com/data/2002/01/17/20020117_175502_ml.htm.

[55] Upheld in *United States* v. *American Library Association*, 539 U.S. 194 (2003).

[56] *Ashcroft* v. *American Civil Liberties Union*, 542 U.S. 656 (2004).

[57] Goldman, Eric (2018) *An Overview of the United States' Section 230 Internet Immunity*, in Giancarlo Frosio (ed.) *Oxford Handbook of Online Intermediary Liability*, at https://ssrn.com/abstract=3306737.

protect Internet service providers (ISPs), even where [a] it was aware of unlawful hosted content; [b] if it had been notified of this by a third party; [c] if it had paid for the data.[58] According to Yen: '[T]he general philosophy motivating these decisions – namely, that the liability against ISPs for subscriber libel would result in undesirable censorship on the Internet – remains vitally important in assessing the desirability of ISP liability.'[59] Despite multiple recent proposals to amend the limited liability safe harbour of s.230 Communications Decency Act to counter 'revenge porn', disinformation and terrorist content, the broad exemption from liability for ISPs has continued into 2020.[60] Frydman and Rorive see courts as 'in line with the legislative intent . . . applied the immunity provision in an extensive manner'.[61]

The second myth that needs exposing is that Europe was entirely reactive to the US Internet liability regime. While it is true that European telecoms were only formally liberalized in 1998, moves to regulate liability for online services predate the public Internet. European consumer Internet use roughly dates to 1998, with the opening of the Telecoms Single Market, and broadband to 2000, with the Local Loop Unbundling Regulation. However, a high-level group of experts led by Professor Luc Soete was set up in May 1995 to advise the European Commission on 'social and societal changes associated with the Information Society', which set out over one hundred initial policy suggestions in January 1996, including the infamous 'bit tax' to prevent e-commerce eroding the local tax base.[62] Among these suggestions was a recommendation to investigate further 'appropriate ways in which the benefits of the Information Society can be more equally distributed between those who benefit and those who lose'. Given the upheavals of the 'zero hours' precariat economy of the 2010s, and the scandals of Apple, Amazon, Alphabet, Facebook and other multinationals' failure to pay tax on in-country activities, the bit tax may be returning in 2020.[63]

In the German Teleservices Act of 1997[64] and *Bavaria* v. *Felix Somm* (Compuserve) case,[65] Germany showed that it wished to see a similar limited liability regime to that in the US. This led with British support to adoption of the

[58] Holznagel, B. (2000) Responsibility for Harmful and Illegal Content as Well as Free Speech on the Internet in the United States of America and Germany, in C. Engel and H. Keller (eds.) *Governance of Global Networks in Light of Differing Local Values*, Nomos: Baden Baden.

[59] Yen, Alfred (2000) Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability and the First Amendment, *Georgetown Law Journal*, Vol, 88, 1.

[60] Holznagel, supra note 58.

[61] Frydman, B. and Rorive, I. (2002) Regulating Internet Content Through Intermediaries in Europe and the USA, *Zeitschrift fur Rechtssoziologie* Bd.23/H1, July 2002, Lucius et Lucius.

[62] CORDIS (1996) *The 'Bit Tax': The Case for Further Research*, at https://cordis.europa.eu/news/rcn/6988/en. The bit tax is a tax on the transmission of information by electronic means – literally, on bits.

[63] Dickson, Annabelle (2018) *UK to Introduce 'Google Tax' in 2020*, Politico, 29 October, at www.politico.eu/article/uk-to-bring-in-digital-services-tax-in–2020/.

[64] Also known as the Information and Communications Services Act (*Informations- und Kommunikationsdienstegesetz – IuKDG*). See IRIS Legal Observations of the European Audiovisual Observatory, IRIS 1997-8:11/16, at http://merlin.obs.coe.int/iris/1997/8/article16.en.html.

[65] Bender, G. (1998) *Bavaria* v. *Felix Somm*: The Pornography Conviction of the Former CompuServe Manager, IJCLP Vol. 1, at www.digital-law.net/IJCLP/1_1998/ijclp_webdoc_14_1_1998.html.

Electronic Commerce Directive of 2000, creating the Digital Single Market in e-commerce. 1999 seems very late in the dot-com boom – but the legislative history of the ECD is directly traceable to 16 April 1997, months before the Teleservices Act was finally ratified. The coordination of US and European lawmaking came in the International Ministerial Conference 'Global Information Networks: Realizing the Potential' in Bonn (then the German capital city) on 6–8 July 1997, which addressed 'international policy-making amongst others for electronic commerce with a view to adopting a Ministerial Declaration'.[66] As with the US Telecommunications Act 1996, it was an eighteenth-month legislative process.

'Safe harbour' protection of ISPs from liability was only implemented on 17 January 2002, when the ECD came into force. Article 12 protects the ISP where it provides 'mere conduit' with no knowledge of, or editorial control over, content or receiver ('does not initiate [or] select the receiver'). Benoit and Frydman establish that it was based on the 1997 German Teleservices Act, albeit with 'slightly more burden on the ISPs in comparison with the former German statute'.[67] Where ISPs provide hosting services, under Article 14, they are protected from liability, in two ways:

1. the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity is apparent; or
2. the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disrupt access of the information.

Like the proverbial three blind monkeys, ISPs and web hosting services should 'hear no evil, see no evil, speak no evil'.[68] As mere ciphers for content, they are protected; should they engage in any filtering of content, they become liable. Thus masterly inactivity except when prompted by law enforcement is the economically most advantageous policy open to them. Frydman and Rorive state 'undoubtedly the Directive seeks to stimulate coregulation'. It does this by formally permitting national courts to override the safe harbour in the case of actual or suspected breach, of national law, including copyright law.

Whereas in the US, the absolute speech protection of the First Amendment and procedural concerns mean that Notice and Take Down is counter-balanced by 'put back' procedures, in Europe, where no such protection of free speech exists, speech freedom is qualified by state rights. In both jurisdictions, Notice and Take Down regimes cause Frydman and Rorive to state that: '[T]his may lead to politically correct or even economically correct unofficial standards that may constitute an

[66] See IP/97/313 Brussels, 16 April 1997: *Electronic Commerce: Commission presents framework for future action*, at http://europa.eu/rapid/press-release_IP-97-313_en.htm?locale=en.

[67] Frydman and Rorive, supra note 61, at 54.

[68] Marsden, C. (2011) Network Neutrality and Internet Service Provider Liability Regulation: Are the Wise Monkeys of Cyberspace Becoming Stupid? *Global Policy*, Vol. 2, No. 1, 1–12.

informal but quite efficient mechanism for content-based private censorship.'[69] It is clear that the economic incentive for ISPs is simply to remove any content notified, otherwise do nothing to monitor content, and let end users, the police and courts, and ultimately the ethics of the content providers decide what is stored and sent over their access networks. Frydman and Rorive state that: 'Business operators should never be entrusted with . . . guidelines defining the limits of the right to free speech and offering procedural guarantees against censorship . . . which belong to the very core of the human rights of a democratic people.'[70] That is nevertheless the situation that ISP Codes of Conduct seek to self-regulate.

Could a stronger case be made to make ISPs responsible for a class of their content, where it serves their commercial benefit? This is an idea that was suggested in the 1990s, before the CDA and ECD supplanted the idea. It has returned in the US with Balkin and Zittrain's concept of information fiduciaries,[71] adapted to Europe in Perrin and Woods' recent work on duty of care.[72]

Vicarious liability tests the ability to benefit and control [i] the right and ability to supervise and [ii] a financial direct interest. This tends to make ISPs choose not to monitor even for law enforcement. The financial direct benefit is interesting in view of the 'killer application' for broadband deployment in the 2000s: Did this include peer-to-peer if the access charges received by the ISP is based on traffic i.e. adverts on portal or bandwidth usage? ISPs arguably benefitted from the existence of copyright infringement on the Internet. Thousands of users desired Internet service precisely because it offers free access to copyrighted materials. As Yen argued, an ISP (like the *Polygram* trade show operator[73]) could make copyright compliance part of its system rules and then monitor for violations.[74] The *Viacom* v. *YouTube* case in 2010 failed to fully establish the burden in such cases.[75]

Similar controversies have arisen beyond content and intellectual property. The landmark 2000 French criminal case of *Yahoo* v. *LICRA*, confirmed that US multinationals must conform to national criminal law on hate speech.[76] With regard to privacy, in 2000, the Europeans and US published the 'safe harbour' agreement.

[69] Frydman and Rorive, supra note 61, at 56.

[70] Ibid at 59.

[71] Balkin, Jack andZittrain, J. (2016) *A Grand Bargain to Make Tech Companies Trustworthy*? The Atlantic, October, https://perma.cc/WW5N-98UZ.

[72] Perrin, W. and Woods, L. (2018) *Harm reduction in social media – what can we learn from other models of regulation?* Carnegie Trust, www.carnegieuktrust.org.uk/blog/harm-reduction-social-media-can-learn-models-regulation/. For criticism, see Smith, Graham (2018) *Take care with that social media duty of care*, Inforrm Blog, 23 October, https://inforrm.org/2018/10/23/take-care-with-that-social-media-duty-of-care-graham-smith/.

[73] *Polygram International Publishing* v. *Nevada/TIG, Inc.*, 855 F. Supp. 1314, 1317-18 (D. Mass. 1994).

[74] Yen, supra note 59, at 19.

[75] *Viacom International, Inc.* v. *YouTube, Inc.*, No. 07 Civ. 2103, US District Court for the Southern District of New York, settled in 2013.

[76] Reidenberg, J. (2005) Technology and Internet Jurisdiction, *University of Pennsylvania Law Review*, Vol. 153, 1951, at http://ssrn.com/abstract=691501.

Negotiated from 1998, it was always legal nonsense if sound policy, and was struck down by the European Court of Justice in *Schrems* in 2015.[77] Its replacement, the 'privacy shield', is equally a sticking plaster over trans-Atlantic differences, and may also be struck down. While this chapter will not describe any of the data protection law developments over the last 25 years, it is noteworthy that the Data Protection Directive[78] was continually attacked as unsuitable for the Internet that it was not expressly designed to regulate,[79] so the new General Data Protection Regulation is already subject to much attack for its failure to regulate artificial intelligence and robotics, yet again technologies for which it was not expressly designed . . . but may be adapted.[80]

## PART 3: THE DEVELOPMENT OF CO-REGULATION

The early period of frenetic legislative activity in 1997–2001 matched the growth of the Internet sector in Europe, which was very small and not officially measured until 1998, when it grew from 9 per cent to over 42 per cent in 2002 in the United Kingdom, for example.[81] This unprecedented growth of a single electronic medium was driven by broadband, mobile and Wifi-enabled Internet access as well as the growth of social media: seven in ten Europeans were using the Internet by 2010.[82] By the end of 2017, 86 per cent of European Union citizens used the Internet, with 433 million users, and 252 million users of Facebook within that number and approximately 400 million Google users.[83]

[77] Case C-362/14.

[78] 95/46/EC.

[79] For which, see the Electronic Privacy Directive 2002/58/EC, which specifically regulates personal data protection on electronic networks.

[80] Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119. See Veale, Michael and Edwards, Lilian (2018) Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling,*Computer Law & Security Review*, Vol. 34, No. 2, 398–404, at http://dx.doi.org/10.2139/ssrn.3071679. See also O'Conor M. (2018) GDPR Is for Life Not Just 25th of May, *Computers and Law*, 18 April, at www.scl.org/blog/10192-gdpr-is-for-life-not-just-the-25th-of-may.

[81] Office of National Statistics (2012) *Internet Access – Households and Individuals, 2012, Figure 1: Households with Internet Access, 1998 to 2012*, at www.ons.gov.uk/ons/rel/rdit2/internet-access–households-and-individuals/2012/chd-figure-1.xls.

[82] OECD (2017) *Digital Economy Outlook*, OECD: Paris, at www.oecd.org/internet/ieconomy/oecd-digital-economy-outlook-2017-9789264276284-en.htm.

[83] Eurostat (2018) *Archive: Internet Access and Use Statistics – Households and Individuals*, Revision as of 15:34, 28 March, at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_access_and_use_statistics_households_and_individuals&oldid=379591.Using a group of various official statistics, the best current source is Internet World Stats (2017) *Internet User Statistics, Facebook & 2017 Population for the 28 European Union member states*, at www.internetworldstats.com/stats9.htm.

The European Commission has conducted continuous monitoring of Internet self-regulation throughout the twenty-first century. A 2004 report for the European Commission concluded:

> An imperfect self-regulatory solution may be better than no solution at all, and we must not raise our standards so high that self-regulation is never attempted. But there are limits to how much imperfection can be tolerated, and for how long. If self-regulatory codes and institutions are insufficiently transparent and accountable, and if they do not observe accepted standards of due diligence, they will lose the trust of the public and fail. There is a danger that some aspects of internet self-regulation fail to conform to accepted standards. We recommend co-regulatory audit as the best balance of fundamental rights and responsive regulation.[84]

The development of Internet regulation has been scrutinized in real time as it developed. Self-regulation continues, and even in the absence of any new laws we would expect the development of the Internet not to be static.[85] Legislative impact assessments of Internet law that ask, 'What happens if we do nothing?', do not involve stasis. The zero option is that the Internet continues to develop.[86] Self-regulation is viewed as making standards and practices across industry that the European Commission, or a Member State, views agnostically in legislative terms (or pre-legislative, given the focus on areas that are emerging and which are not yet regulated), but which intends to monitor to analyse the extent to which the self-regulation approaches the standards of 'representativeness' that co-regulation is meant to demonstrate as a best practice. The Commission's insistence that this is not an inevitable journey is backed by its actions in such areas as technical standard setting.

The largest European Internet companies are United States based. Half of the world's ten largest public companies by capitalization are computer technology, Internet-based advertising, media and e-commerce conglomerates: Google (trading as Alphabet Inc.), Apple, Facebook, Amazon, and Microsoft (GAFAM). Apple is in the global top twenty corporations by revenues, with two Internet access providers in the top thirty (AT&T and Verizon). Large Internet companies have very high profit margins driven in part by their avoidance of high sales taxes, corporate taxes and transfer pricing, as well as merger activity. The European Commission explained

[84] Directorate-General for Communications Networks, Content and Technology (European Commission), Programme in Comparative Law and Policy (2004) *Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis*, Final Report of IAPCODE Project for European Commission DG Information Society Safer Internet Action Plan, 30 April, Section 12.7, at https://publications.europa.eu/en/publication-detail/-/publication/b7c998d9-75d6-464d-9d91-d59aa90a543c/language-en.

[85] Marsden, C. (2017) *How Law and Computer Science Can Work Together to Improve the Information Society: Seeking to remedy bad legislation with good science*, Communications of the ACM, Viewpoint: Law and Technology.

[86] Marsden C., Cave, J. and Simmons, S. (2008) *Options for and Effectiveness of Internet Self- and Co-Regulation*, TR-566-EC. Santa Monica, CA: RAND Corporation.

that: 'Google's search engine has held very high market shares in all EEA countries, exceeding 90% in most. It has done so consistently since at least 2008.'[87] Regulation by states of the failings of those private actors is in general much slower, with the Google competition breach investigated from November 2010 until a record fine was finally issued in June 2017. The actors that enforce regulation on the Internet are thus young but globally successful multinationals, an unprecedented group of private actors regulating speech and commerce on a communications medium. In 2017, the European Commission found all these companies guilty of anticompetitive conduct:

- Apple in Ireland, and Amazon in Luxembourg, had received illegal state aid of respectively €13 billion and €1.5 billion.
- Google abused its dominance through its search business, EC imposing a €2.4 billion fine.
- Facebook had flagrantly breached the terms of its merger with WhatsApp in 2014, with an EC fine of €110 million imposed in May 2017.
- Previously dominant software and Internet company Microsoft had been found guilty of abusing its dominance three times since 2007; fined a total of €2.2 billion.

This total of fines is a record for any sector, as are the individual instances of fines. To give a sense of the scale of mergers by the companies in that period, they made 436 acquisitions worth a total $131 billion in the decade to June 2017.[88] These private actors operate with enormous scale and scope, yet they are legally regulated exactly as small commercial websites. The size and scale of their operations make their regulation more difficult than the equivalents in other industries – for instance, the infamous 'Seven Sisters' energy companies whose regulation inspired both energy and, to some extent, environmental law.[89] Such regulation between states and firms has been termed 'para-diplomacy',[90] and it is constantly engaged in by the GAFAM group.

Major platforms (now including Google, Yahoo!, Facebook, Microsoft) and access providers formed a self-regulatory group, the Global Network Initiative (GNI), in 2008 to respond to government demands for better enforcement. GNI members publish transparency reports which can be audited by the board of GNI,

[87] European Commission (2017) Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service, Factsheet, Brussels, 27 June 2017, at http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm.

[88] European Commission (2017) Speech by Johannes Laitenberger, Director-General for Competition, *EU competition law in innovation and digital markets: fairness and the consumer welfare perspective*, at http://ec.europa.eu/competition/speeches/text/sp2017_15_en.pdf.

[89] Sampson, Anthony (1973) *The Sovereign State of ITT*, New York: Stein and Day.

[90] Stopford, John and Strange, Susan (1991) *Rival States, Rival Firms*, Cambridge: Cambridge University Press; Duchacek, Ivo D. (1984) The International Dimension of Subnational Self-Government, *Publius: The Journal of Federalism*, Vol. 14, No. 4, 5–31, at https://doi.org/10.1093/oxfordjournals.pubjof.a037513.

an example of self-regulation by a group.[91] Google first published a report in 2010, and reported in 2018 almost 4 billion annual copyright removal requests as compared to 495,000 annual "right to be forgotten" delisting requests and only 16,000 annual government content requests (affecting 221,000 websites), demonstrating that its most substantial enforcement actions are carried out on behalf of copyright owners.[92] Facebook, Twitter (since 2012), Amazon (since 2015) and others also produce annual transparency reports.[93]

Co-regulation was noted by United States Congress in 2002 to describe certain aspects of European regulation: 'government enforcement of private regulations'.[94] It actually came from Australia.[95] The European adventure in co-regulation in wider consumer protection legislation, as well as standards setting, was made detailed in 2002,[96] and became official policy in December 2003, with the Inter-Institutional Agreement on Better Law-Making (IIA), which defines co-regulation.[97] Although a non-legislative act, the IIA is virtually a constitutional document in European law, and its importance cannot be over-estimated, as it agrees the rules of engagement of the European Parliament, Council of Ministers and Commission.[98] The Commission confirms that forms of regulation short of state regulation 'will not be applicable where fundamental rights or important political options are at stake or in situations where the rules must be applied in a uniform fashion in all Member States'.

De jure co-regulation involves legislation that tells the industry 'regulate or else'. The UK *Digital Economy Act 2010* included two specific elements of co-regulation, for the domain name authority (Nominet) and audiovisual media services online (the Authority for Television on Demand). De facto co-regulation exists where the regulators have used their powers of extreme persuasion. It is an area in which the industry players are very aware that the regulator has power. There can be de facto co-regulation taking place alongside de jure co-regulation.

The Commission in 2005 analysed co-regulation in terms of 'better regulation'.[99] This was immediately made part of internal EC practice in the Impact Assessment

[91] Global Network Initiative (2018) *2017 Annual Report*, at https://globalnetworkinitiative.org/global-network-initiative-annual-report-2017-reinforcing-a-global-standard/ and https://globalnetworkinitiative.org/about-gni/.

[92] https://transparencyreport.google.com/copyright/overview – noting many companies have such reports, linking to 42 others (some have since merged or discontinued reports).

[93] See, for instance, https://transparency.twitter.com/ and https://aws.amazon.com/blogs/security/privacy-and-data-security/.

[94] H. Rept. 107–803 – *Legislative Review Activities of the Committee On International Relations* 107th Congress (2001-2002). See, generally, for US Internet co-regulation, Weiser, P. (2009) The Future of Internet Regulation, *U.C. Davis Law Review*, Vol. 43, 529–90.

[95] Marsden, *Internet Co-Regulation*, supra note 12.

[96] See COM/2002/275, COM/2002/0278, COM 2002/704.

[97] Inter-Institutional Agreement on Better Law-Making (OJ C 321, 31.12.2003), pp. 1–5.

[98] European Union (2016) *Better Regulation*, at www.consilium.europa.eu/en/policies/better-regulation/.

[99] COM/2005/97.

Guidelines,[100] which the Commission must follow before bringing forward a new legislative or policy proposal.[101] Price and Verhulst (2005) contained significant focus on AOL and internal self-organization.[102] They identified even then increasing realism in recognizing competition problems, emerging monopolies, and dominance. Verhulst and Latzer provided excellent analysis of the types of co-regulation beginning to develop and their institutional path dependency.[103] They identify five types of regulation, short of statutory agency-led regulation:

- Co-regulation,
- State-supported self-regulation,
- Collective industry self-regulation,
- Single company self-organization,
- Self-help/restriction by users including rankings to impose restrictions on access to content.

Note the direction of travel: both bottom-up transformations from self- into co-regulatory bodies, and top-down delegation from regulation into co- but not self-regulation. Also note examples of 'zombie' self-regulation – where no one will declare the patient dead or switch off the life support machine. I described these as 'Potemkin' self-regulators, where there was a website and the appearance of a regulator but few resources, no physical address containing offices and little or no apparent adjudication and enforcement.[104] We should note the gains and losses in the lifecycle of regulation – will self-regulation ossify if it stays true to its principles of self-regulation? If ossification were to result, would it matter other than to self-regulatory purists if a mature self-regulator were then to be made into a co-regulator? UK converged communications regulator Ofcom's own managerial and regulatory analysis of co- and self-regulation arrives at similar conclusions.[105]

The EC has made it pragmatic to fund standards and ex ante support self-regulation in cases where the US would simply ex post regulate via competition law. This leads to substantial US–European differences of approach, which may create 'transatlantic competition of standardization philosophies . . . [in] consumer protection systems'.[106]

[100] SEC /2005/791.

[101] This is now codified in the new Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making OJ L 123, 12.5.2016, pp. 1–14, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:123:FULL&from=EN.

[102] Price M. and Verhulst, S. (2005) *Self-Regulation and the Internet*, Amsterdam: Kluwer.

[103] Latzer, Michael, Price, Monroe E., Saurwein, Florian, Verhulst and Stefaan G. (2007) *Comparative Analysis of International Co- and Self-Regulation in Communications Markets*, Research report commissioned by Ofcom.

[104] Marsden, *Internet Co-Regulation*, supra note 12, at pp. 60, 147, 222.

[105] Ofcom (2008) *Identifying Appropriate Regulatory Solutions: Principles for Analysing Self- and Co-Regulation*, 10 December.

[106] Newman Abraham, L. and Bach,David (2004) Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States, *Governance: An International Journal of Policy, Administration, and Institutions*, Vol. 17, No. 3, July 2004, 388.

Examples of co-regulation have become frequent in this field in the 2000s, notably in data privacy, domain name governance, content filtering, Internet security, and network neutrality, as well as standard setting and social network privacy regulation.[107] Both soft law and soft enforcement play a vital regulatory role which legal positivists would be in danger of overlooking by a failure to consider the law in its co-regulatory context.

A Beaufort scale of co-regulation was developed for the European Commission based on the Beaufort scale of wind speed (from calm to hurricane).[108] The wind in this case is the degree to which the government was breathing on the forms of self-regulation that were taking place. Zero was a state of calm, which would be an entirely technical standards body whose standards were formed totally within the technical community, such as the Internet Engineering Task Force, up to a state of storm, which could be the forms of co-regulation that were formalized in the Digital Economy Act. Between zero and eleven, there is a lot of room for us to see different elements of influence that have been exerted. That wind is blowing a lot more strongly from European governments and from parliaments towards trying to achieve something much closer to co-regulation than to self-regulation. There are three alternatives:

1. not to regulate, but the world develops without regulation
2. to regulate all the platforms that legislators are concerned about
3. to regulate only the dominant platforms.

It is this regulatory dilemma that I consider in the final part of the chapter.

## PART 4: BACK TO THE FUTURE OF CYBERLAW IN THE UBIQUITOUS NETWORKED COMPUTING ERA

Internet lawyers are widening their horizons and returning to the broader notion of being information lawyers whose interests extend beyond a public IP network. The end of the special place for Internet law, and its absorption into media law, has been prematurely announced. It is not only the European institutions that are becoming excited about more Internet regulation, driven in part by self-preservation and the rise of disinformation ('fake news' – sic). Reed and others question how we regulate AI[109] and dominance of the 'surveillance-industrial' state in these post-Snowden /Schrems/GDPR times, pushing digital law into even constitutional studies.[110] These are exciting times to be an information lawyer.

[107] Froomkin, A. Michael, Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, *Duke Law Journal*, Vol. 50, 17, at www.law.miami.edu/~froomkin/articles/icann.pdf.

[108] Marsden, Cave and Simmons, supra note 86.

[109] Reed, Chris (2018) *How Should We Regulate Artificial Intelligence?* Philosophical Transactions of the Royal Society, A 2018 376 20170360.

[110] See, for instance, Frischmann, Brett M. (2005) An Economic Theory of Infrastructure and Commons Management, *Minnesota Law Review*, Vol. 89, 917–1030, https://ssrn.com/abstract=588424.

To put a damp squib on too much recurrent techno-optimism or cynicism, I argue that most arguments for regulating the Internet and cyber-technologies today remain old wine in new bottles.[111] The United Kingdom regulator Ofcom has called for more regulation, and potentially a new regulator, of the Internet.[112] Most developed legal systems have lots of legal regulators of information, even if none of those is entirely shiny, new, and 'cyber'. There is the UK Information Commissioner, Electoral Commission, Ofcom itself, the Advertising Standards Authority, and others. There are technical support institutions such as National Cyber Security Centre,[113] and a variety of non-governmental organizations such as the Nuffield Foundation-supported Ada Lovelace Foundation, the Turing Institute, and venerable Foundation for Information Policy Research.[114] In constructing what I call 'OffData', a regulator of electronic communications and content,[115] we need to learn the lessons of previous regulatory mergers both inside (OfCom) and outside (OfGem) communications. We need to recall what is known about sectoral regulation. UK Ofcom was set up almost twenty years ago as a result of technological convergence between broadcasting and telephony,[116] but deliberately constructed not to regulate Internet content. It is now required to so do. This is not a moment for unique solution peddling or an ahistorical view of the need to extend competences beyond a privacy, a security, a sectoral competition, and a communications regulator.

While information law is maturing, and the old Internet law/cyberlaw nomenclature may be fading, what we do as lawyers dealing with computers and their impact on society is growing more important. Some of the new ideas about regulating the Internet and artificial intelligence (AI) betray a naive faith in technology companies' intentions towards law enforcement. It is now the job of grizzled, veteran information lawyers to help policy makers understand how to make better laws for cyberspace.[117] Hildebrandt explains the scale and scope that can create disinformation problems in social media platforms:

[111] Marsden, C. (2018) *Oral Evidence to Lords Communications Committee, "The internet: to regulate or not to regulate?"* Parliamentlive.tv, 24 April, at https://parliamentlive.tv/Event/Index/4fac3ac3-3408-4d3b-9347-52d567e3bf62.

[112] White, Sharon (2018) *Tackling online harm – a regulator's perspective*: Speech by Sharon White to the Royal Television Society, 18 September, at www.ofcom.org.uk/about-ofcom/latest/media/speeches/2018/tackling-online-harm.

[113] Merging CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

[114] See www.cl.cam.ac.uk/~rja14/fipr-20th.html.

[115] Marsden, C. (2018) Prosumer Law and Network Platform Regulation: The Long View Towards Creating Offdata, *Georgetown Technology Law Review*, Vol. 2, No. 2, pp. 376–98.

[116] Oftel (1995) *Beyond the Telephone, the TV and the PC*: Consultation Document. Note further consultations were released, the last in 1998 – seen as a forerunner to the agenda on convergent communications for government and eventually Ofcom. See Barnes, Fod (2000) Commentary: When to Regulate in the GIS? A Public Policy Perspective, chapter 7, pp. 117–24 in Marsden, C. ed. (2000) *Regulating the Global Information Society*, New York: Routledge.

[117] See Kroll, Joshua A., Huey, Joanna, Barocas, Solon, Felten, Edward W., Reidenberg, Joel R., Robinson, David G. and Yu, Harlan (2017) Accountable Algorithms, *University of Pennsylvania Law Review*, Vol. 165, at https://ssrn.com/abstract=2765268. See also Reed, supra note 2.

> Due to their distributed, networked, and data-driven architecture, platforms enable the construction of invasive, over-complete, statistically inferred, profiles of individuals (exposure), the spreading of fake content and fake accounts, the intervention of botfarms and malware as well as persistent AB testing, targeted advertising, and automated, targeted recycling of fake content (manipulation).[118]

Some of the claims that AI can 'solve' the problem of disinformation ('fake news') do just that. Limiting the automated execution of decisions (e.g. account suspension) on AI-discovered problems is essential in ensuring human agency and natural justice: the right to appeal. That does not prevent Internet platform operators' suspension of 'bot' accounts at scale, but ensures the correct auditing of the system processes deployed.[119]

Technological solutions to detect and remove illegal/undesirable content have become more effective, but they also raise questions about who is 'judge' in determining what is legal/illegal, desirable/undesirable in society. Underlying AI use is a difficult choice between different elements of law and technology, public and private solutions, with trade-offs between judicial decision making, scalability, and impact on users' freedom of expression. Public and private actors have suggested that AI could play a larger role in future identification of problematic content – but these systems have their own prejudices and biases. It is worth restating that neither law nor technology is neutral: they both embody the values and priorities of those who have designed them ('garbage in, garbage out').

Does the use of AI that employs algorithmic processes to identify 'undesirable' content and nudge it out of consumers' view, provide a means for effective self-regulation by platforms? The UK Parliament Artificial Intelligence Committee reported on some of these issues in 2017.[120] There are an enormous number of false positives in taking material down. It is very difficult for AI to tell the difference between a picture of fried chicken and a Labradoodle, simply because of the nature of the attempts by algorithms to match these things.[121] It will need human intervention to analyse these false positives. AI can be deployed, but Google and Facebook are employing 50,000 more people because they recognize that there will have to be a mixture in

[118] Hildebrandt, Mireille (2018) Primitives of Legal Protection in the Era of Data-Driven Platforms, Georgetown Technology Law Review, Vol. 2, 252, at 253 footnote 3.

[119] See Marsden, Chris and Meyer, Trisha (2019) Regulating Disinformation with Artificial Intelligence (AI): The Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism, Report for Panel for the Future of Science and Technology (STOA), Scientific Foresight Unit of the Directorate for Impact Assessment and European Added Value, Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

[120] House of Lords (2017) *AI Select Committee: AI Report Published*, at www.parliament.uk/business/committees/committees-a-z/lords-select/ai-committee/news-parliament-2017/ai-report-published/ (note the report is published in non-standard URL accessed from this link).

[121] Reddit poster (2017) *Artificial Intelligence Can't Tell Fried Chicken from Labradoodles*, at www.reddit.com/r/funny/comments/6h47qr/artificial_ intelligence_cant_tell_fried_chicken/.

order to achieve any kind of aim.[122] Artificial intelligence and algorithms cannot be the only way to regulate content in future.[123]

'Mechanical Turks' are people employed – subcontracted, typically – to carry out these activities,[124] in parts of the world where their own cultural understanding of the content they are dealing with may not be ideal.[125] One of the problems is that they are responding to a perceived need to remove more content, rather than addressing fair process and due process. Subcontracting to people on very low wages in locations other than Europe is a great deal cheaper than employing a lawyer to work out whether there should be an appeal to put content back online. The incentive structure will be for platforms to demonstrate how much content they have removed.

Transparency and explanation are necessary, but remain a small first step towards greater co-regulation.[126] Veale et al. have explained how to move beyond transparency and explicability to replicability: to be able to run the result and produce the answer that matches the answer they have.[127] The greater the transparency, the greater the amount of information you give to those users who do not read the terms of service online: the degree to which that helps is limited. Prosumers are told: 'If you do not agree to the effectively unilateral terms of service you may no longer use Facebook.' A better approach would be the ability to replicate the result achieved by the company producing the algorithm. Algorithms change all the time, and the algorithm for Google search, for instance, is changed constantly. There are good reasons to keep that as a trade secret. Replicability would be the ability to look at the algorithm in use at the time and, as an audit function, run it back through the data to produce the same result. It is used in medical trials as a basic principle of scientific inquiry. It would help to have more faith in what is otherwise a black box that prosumers and regulators have to trust. The European Commission has used the overarching phrase 'a fair deal for consumers'.[128]

[122] www.fastcompany.com/40563782/how-a-i-anxiety-is-creating-more-jobs-for-humans.

[123] Discussed by Marietje Schaake MEP in April at www.theguardian.com/commentisfree/2018/apr/04/algorithms-powerful-europe-response-social-media.

[124] Hara, Kotaro, Adams, Abi, Milland, Kristy, Savage, Saiph, Callison-Burch, Chris and Bigham, Jeffrey (2017) *A Data-Driven Analysis of Workers' Earnings on Amazon Mechanical Turk*. arXiv:1712.05796, Conditionally accepted for inclusion in the 2018 ACM Conference on Human Factors in Computing Systems (CHI'18) Papers program.

[125] YouTube Transparency Report (2018), at https://transparencyreport.google.com/youtube-policy/overview.

[126] Edwards, Lilian and Veale, Michael (2017) *Slave to the Algorithm? Why a "Right to Explanation" is Probably Not the Remedy You are Looking for*, at https://ssrn.com/abstract=2972855; Erdos, David (2016) European Data Protection Regulation and Online New Media: Mind the Enforcement, *Gap Journal of Law and Society*, Vol. 43, No. 4, 534–64, at http://dx.doi.org/10.1111/jols.12002.

[127] Veale, Michael, Binns, Reuben and Van Kleek, Max (2018) *The General Data Protection Regulation: An Opportunity for the CHI Community?* (CHI-GDPR 2018), Workshop at ACM CHI'18, 22 April 2018, Montreal, Canada, arXiv:1803.06174.

[128] Vestager, M. (2018) *Competition and a Fair Deal for Consumers Online*, Netherlands Authority for Consumers and Markets Fifth Anniversary Conference, The Hague, 26 April, at https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-and-fair-deal-consumers-online_en.

Platform regulation is a new version of an existing regulated problem, with potentially dramatic negative effects on democracy and media pluralism.[129] In tackling disinformation (and other undesirable uses of online communication, as the history of electoral and defamation reform shows), not only the effectiveness of the technological measures needs to be considered, but also raising awareness of the individual and social responsibility for the provision and appreciation of verifiable truthful content, by independent platforms rather than a single central authority. Media pluralism and literacy go hand in hand with any technological intervention.

I predict that 2020 will see the implementation of hard law requiring 'notice and action' within one hour of complaints about illegal content online.[130] The vigorous action on social network regulation has not happened, in spite of urging from national and European politicians in view of terrorist content, sexual abuse, fake news, and the other vile elements of human society manifested on the Internet. European regulators continue to rely more on corporate social (ir)responsibility than hard law. The European Commission record fine for Google is being appealed, but it will have to accept some kind of co-regulation of its vertically integrated advertising in time.

I explained in the Introduction to this chapter that Werbach's Digital Tornado, along with Reidenberg's conception of *lex informatica*, heralded a model of limited state but very substantial responsible collective self-regulation. Hard law, in the shape of the proposed European Digital Services Act to be introduced in 2020, will continue in the 2020s to be accompanied by Codes of Conduct and other self- or co-regulatory measures. At the time of writing, the world was plunging into a deep economic and social depression due to the pandemic, with broadband connectivity and Internet platforms ever more vital. Even as legislatures introduce hard law to combat their particular favourite online harm, continued emphasis will focus on giant platforms' self-regulatory practices. Cyberlaw has become mainstream in the most dramatic manner imaginable.

[129] A recent Bird & Bird study for the European Commission evaluated the first triennial review of Net Neutrality in Regulation 2015/2120 – its conclusions were that the lack of enforcement to date means it is too early to tell how useful it will be. But zero rating is more controversial in developing nations, not least because the use of zero rated WhatsApp in data-poor Brazil appears to have helped swing the Presidential election of Bolsonaro: Belli, Luca (2018) *WhatsApp Skewed Brazilian Election, Proving Social Media's Danger to Democracy*, The Conversation, 5 December, at https://theconversation.com/whatsapp-skewed-brazilian-election-proving-social-medias-danger-to-democracy-106476.

[130] Marsden, C. (2019) *Predictions 2019: Professor Chris Marsden*, Society for Computers and Law, at www.scl.org/articles/10379-predictions-2019-professor-chris-marsden.