TAMING THE WILD WEST: GOVERNMENT AND THE INTERNET

THE DAVID VAUGHAN CBE QC ANNUAL ANTITRUST LITIGATION LECTURE
CLIFFORD CHANCE, 14 NOVEMBER 2019

DAVID ANDERSON
(LORD ANDERSON OF IPSWICH KBE QC)

INTRODUCTION

1. I remember some of the first words that David Vaughan spoke to me, in 1986, manuscript in hand: he a relatively new silk at Brick Court Chambers, I an eager mini-pupil:

   > "Could you possibly … copy this out in your best handwriting and take it down to ICI?"

2. I later came to know David as an enthusiastic early adopter of new technology, commandeering his instructing solicitors' brick-like carphones to call Lesley and the children, delightedly, from every corner of Europe and beyond. But his first request to me could have been given by Chaucer's Man of Law, if for ICI we substitute an alchemist practising at Millbank; and it struck me even at the time as quaint. I was fresh from Washington DC, where as a young lawyer I had been treated not only to my own electric typewriter but to a secretary who knew how to use the fax machine. London, it seemed, was a little slow in joining the modern world.

3. David's handwriting was never easy: in the words of Somerville and Ross: "*No individual word was decipherable, but with a bold reader, groups could be made to conform to a scheme based on probabilities.*"[1] But on closer inspection, the significance of the

[1] Edith Somerville and Martin Ross, *In Mr Knox's Country* (1915).

document for which my services in the Brick Court scriptorium had been requested became clear: on it were written David's first thoughts for ICI's appeal against the Commission's finding that it had participated in a polypropylene cartel, and the imposition of a then unimaginably large fine of 10 million ECU.[2]

4. That appeal was eventually lodged in Luxembourg, taking advantage of the 10-day "extension on account of distance" that the rules used to provide for. Those based in Brussels had a 1-day extension, as I remember: from New York or Tokyo, it was 30 days. As Sir Jeremy Lever once remarked, the extension periods seem to have been calculated on the assumption that pleadings would be delivered to Luxembourg by barge.

5. From an educational as well as a financial point of view I have much cause to be grateful to ICI for that cartel; for its counterparts in PVC and low-density polyethylene; and for the global market-sharing agreement with Solvay in soda ash, said by the Commission to have continued unbroken since 1945, on which 22 years of litigation were eventually brought to an end by a judgment of the Grand Chamber of the Court of Justice in October 2011.[3]

6. But deterred by the joyless task of cross-examining economists, and diverted into other legal interests, my involvement in antitrust litigation has become infrequent in recent years. So with the kind permission of Clifford Chance I will be attempting in this lecture something a little broader: some reflections on the role of Government in the Internet age. If this lecture were a website it would be a beta version: so I welcome comments and criticisms as well as questions.

[2] Commission Decision 86/398/EEC: 1986 OJ L230/1.
[3] Case C-110/10P.

A CHANGING WORLD

7. The internet reached Brick Court Chambers in the 1990s, though without any effect on the stately pace of litigation that I have just described. So far as I recall, we early pioneers used our dial-up modems principally to participate in online forums and slow-motion banter with each other on the subject of Championship football.

Early Utopianism

8. Across the Atlantic, broader horizons beckoned. John Perry Barlow was a cattle rancher raised in Wyoming, who became a Grateful Dead Lyricist and Harvard Fellow. He was reacting to the Communications Decency Act of 1996, which prohibited the transmission over the internet of indecent sexual images to under 18s, when he launched his "*Declaration of the Independence of Cyberspace*" with the famous words:

> "Governments of the industrial world, you weary giants of flesh and steel … You are not welcome among us. You have no sovereignty where we gather.
> …
> We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different."

Barlow referred to the internet as an "*electronic frontier*", which like the American West should be left to its inhabitants to govern as they please. Though he died last year, his Electronic Frontier Foundation, based in San Francisco, remains a leading defender of digital privacy, free speech and innovation.

9. About the exciting potential of the internet, Barlow was surely right. I used to carry a diary in my jacket pocket, of about this size – and I still

do. But if I may slip into 20th century language, this modern, electronic diary is also a telephone, a calculator, an alarm clock, a camera, a video camera. It is a wallet, a bank branch, a whole shelf of photo albums, a gaming console, a map and street atlas that shows my position. A weather forecaster, a journey planner, a translation service, a news-stand with the latest papers from around the world, a radio, a television, a music centre playing all the music in the world. It is a library, a bookshop, a general store that is never out of stock, an emailer and messaging service, a typist who takes dictation, a personal assistant (though Siri is a little slow on the uptake sometimes), and a tracker of other, similar objects. Most wonderfully of all, it connects me continuously to family, friends and communities with the same interests; to the whole sum of human knowledge and experience in written, graphic and moving image form; and – a plug here for my favourite platform, Twitter – to the real-time thoughts and writings of as many of the cleverest, funniest and most interesting people in the world as I choose to follow. All this at remarkably moderate cost – at least in money.

10. And miraculous though it may seem to those of us who grew up in an analogue world, all this is merely a taken-for-granted baseline for younger generations who in years to come will reap the benefits of unlimited and instantaneous data transfer in terms of autonomous transport, interconnected appliances, virtual reality, assisted memory and all the applications that human ingenuity – or indeed the ingenuity of artificial intelligence – are yet to devise.

11. We are, in short, at the start of an information revolution like none we have seen before: on that I stand unapologetically with Barlow – and indeed with the poet Wordsworth, who said of the French Revolution, "*Bliss was it in that dawn to be alive*."[4]

[4] William Wordsworth, *The Prelude*.

The state strikes back

12. Of course, like all revolutions, this one has the potential not only for good things but for profound disruption and harm. Barlow recognised that cyberspace would throw up problems but thought they could be addressed by its users, by their own means, without the intervention of governments.

13. His ideas received some remarkable early support in the 1997 decision of the US Supreme Court in *Reno v ACLU,*[5] which by 7-2 declared the indecency provisions of the Communications Decency Act to be an unconstitutional abridgement of the First Amendment right to free speech. Justice John Paul Stevens wrote for the Court that the internet was "*a unique medium – known to its users as 'cyberspace' – located in no particular geographical location but available to anyone, anywhere in the world.*" It contained, he said, "*vast democratic fora*" that have not "*been subject to the type of government supervision and regulation that has attended the broadcast industry.*" In the words of Justice Sandra Day O'Connor, like Barlow brought up on a remote western ranch: "*The electronic world is fundamentally different.*"

14. But this turned out to be the high water mark of the law's deference to cyber-exceptionalism. In their classic book "Who Controls the Internet?", published in 2006, law professors Jack Goldsmith and Tim Wu told the story of the subsequent decade. They answered their own question in a decisive if unromantic way: national governments control the internet, and must continue to do so.[6] They made three observations.

    a. First, contrary to some initial expectations, national governments turned out to have effective ways of enforcing their laws against

[5] *ACLU v Reno* 521 US 844 (1997).

[6] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, OUP 2006.

internet communications, even when they originated elsewhere. Geo-blocking, once said to be impossible, had become commonplace.

b. Secondly, reflecting these pressures but also the demands of individuals in different places, the internet – or splinternet – was beginning to look different in countries "*separated by walls of bandwidth, language and filters*".

c. Thirdly, this geographically bordered internet had many virtues. Companies engaged in internet commerce need to be plugged into a reliable legal system. Most citizens want their governments to prevent internet harms, wherever they originate. And as illustrated by the campaign for net neutrality – the equal treatment by internet service providers of all internet communications –governments can help protect "*the original, unpredictable, and uncontrolled nature of the internet*".[7]

So the death of the 1990s vision of the internet should be mourned, concluded Goldsmith and Wu, but only a little. As the internet moves out of its adolescent period, increasing numbers agree. In a Washington Post op-ed earlier this year, even Mark Zuckerberg – he of the motto "*Move fast and break things*" – called for regulation in the areas of harmful content, election integrity, privacy and data portability.

15. So Barlow's "*weary giants of flesh and steel*" have a place in cyberspace. But what form that presence should take is a highly contested question. Nor should we assume that the right answers will be quickly found, any more than they were during the last industrial revolution which, fuelled by the steam engine, transformed the economy, transport, communications, global relations, politics,

[7] *Ibid.*, Preface to the paperback edition (2008).

living conditions and so much else during the 18th and 19th centuries. As the MP Liam Byrne likes to point out, it took many decades, and many Factories Acts, before the new technologies were regulated in such a way as to provide for a "*just transition*".[8]

16. The interfaces between government and the internet are far too many to deal with in a single lecture. So I will address just a few current issues – taking as my starting point the most significant way in which the landscape has changed in the past 20 years.

EMERGENCE OF THE TECH GIANTS

17. That is of course the emergence of giant tech companies. At over 3 trillion US dollars, the combined market capitalisation of Facebook, Apple, Amazon, Netflix and Google – the so-called FAANGS – is greater than the entire economies of France or the UK. Yet with the exception of Apple, whose business model is based on the sale of its products, none of these giant corporations even existed as a public company when John Perry Barlow was writing in 1996.

Scale

18. The breathtaking speed of their rise is illustrated by the fact that when the 19-year-old Mark Zuckerberg launched Facebook in February 2004, Roger Federer was already the world's no. 1 tennis player. Facebook now boasts some 2.5 billion monthly active users: in recent years it purchased WhatsApp with an estimated 1.5 billion and Instagram with more than 1 billion monthly active users. Its dominance in social media is echoed by the influence of Amazon in online retail, and of Google in online search. Google and Facebook alone account for more than half the world's *digital* advertising

[8] See, e.g., HC Deb 3 October 2019, c414WH.

spend, itself the majority of *total* advertising spend in many developed countries.

Scope

19. And these companies are diversifying. Google and its parent company Alphabet continue to derive most of their money from advertising: but after some 200 acquisitions their stable includes video-sharing site YouTube, the Android operating system used in most of the world's smartphones and tablets, and ventures in genomics, healthcare and self-driving cars. Amazon has been described as not just a retailer but "*a marketing platform, a delivery and logistics network, a payment service, a credit lender, an auction house, a major book publisher, a producer of television and films, a fashion designer, a hardware manufacturer and a leading host of cloud server space*".[9]

Surveillance capitalism

20. As significant as their scale and their scope is the business model to which most of these companies operate: "*surveillance capitalism*", to use the term popularised in Shoshana Zuboff's recent book of that name.[10]

21. Her starting point is to explain that Google, Facebook, Amazon, eBay and so on are free to those of us who use them because we are not really their *customers* but their *raw materials*. Our value to them is in the personal data that they obtain from us every time we confide to them our *feelings* by posting on their platforms, our *interests* by using their search engines or visiting other websites that contain their

[9] Lina Khan, "Amazon's Antitrust Paradox"(2017) Yale Law Journal 126:710.

[10] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019). A useful short summary is Graham Greenleaf, "Elements of Zuboff's surveillance capitalism", Privacy Laws & Business, August 2019, p.29.

cookies, and our *material wants* by our browsing on their online retail and auction sites.

22. As we use a platform to connect with our friends or ease the day-to-day business of our lives, that platform is harvesting personal data that is not required for the purpose of the transaction we have performed. This so-called behavioural surplus constitutes the payment – Zuboff would say the over-payment – that we make for the service provided.

23. Big tech maximises and aggregates our personal data. It uses techniques of behavioural analytics to predict, to monetise, to influence and ultimately even to determine what we buy, where we go and how we vote. Zuboff's surveillance capitalism is a dystopian ideology of docile consumerism: not so much Orwell's surveillance state as Huxley's Brave New World.

24. The book exemplifies what the solicitor Graham Smith, a long-time observer of the internet, has aptly described as "*a lurch from extreme optimism to extreme negativity*".[11] Zuboff spends little time discussing what can government do to mitigate the effects of surveillance capitalism.

25. She finds though a glimmer of hope in the EU's General Data Protection Regulation (GDPR). She has in mind, perhaps, the strong enforcement of its data minimisation principle, which requires that data are "*limited to what is necessary in relation to the purposes for which they are processed*", and of the new accountability principle that requires compliance to be demonstrated. That and public indignation, she hopes, might help. We shall see.

[11] Graham Smith, "The internet: broken or about to be broken?", Keynote Speech to the SCL Annual Conference 2019, SCL blog 9 October 2019.

GOVERNMENT SURVEILLANCE

26. Switching dystopias from Huxley to Orwell, I want to touch now on the role of big tech in *Government* surveillance of the internet. That relationship is particularly close in China, where data gathered in "*smart cities*" by the giant companies Baidu, Alibaba and Tencent is fed into the developing system of "*social credits*", under which citizens are scored for their behaviour and subject to controls, determined by their scores, on how they can travel and where they can live. But Edward Snowden revealed that there was cooperation in western countries as well, though for less sinister purposes. Partly as a consequence, this remains a delicate and contested area.

CLOUD Act Treaty

27. In the old days, when electronic communication meant a telephone call, for UK law enforcement to intercept the line was a relatively simple matter. A warrant would be obtained from the Home Secretary and served on BT, or a domestic mobile provider, which complied as a matter of legal obligation.

28. Things got more complicated when even domestic communications started to be conducted over internet platforms, often based in the United States. Cross-border requests, even if related to purely domestic crimes, required use of a cumbersome mutual legal assistance treaty (MLAT) which took many months. This could still be useful for securing evidence, but was too slow to be useful in fast-moving investigations.

29. The Investigatory Powers Act 2016 introduces a double lock: warrants are not only authorised by the Secretary of State, as in the past, but approved by serving or retired senior judges: the judicial commissioners of the new oversight body, IPCO.

30. That upgrade of protections helped pave the way first for an enabling Act of Congress, the CLOUD Act of 2018, and then for the first Treaty to be made under it: a US-UK Treaty, announced last month, which will enter into force once scrutinised by Congress and by Parliament.

31. Though reciprocal, the Treaty will be particularly helpful to UK law enforcement. British serious crime warrants concerning non-US citizens will be enforceable against US platforms in just the same way as if they had been issued by the FISA Court for the FBI.

32. That exercise in mutual recognition will be a model for further US agreements, initially with the EU and Australia. It will go some way to restoring a capability that was lost when communications migrated to the internet. More broadly, it is a reminder that in a world where crime knows *no* boundaries and business increasingly *few*, national governments need to cooperate if they are to keep up. A lesson that governments need to learn if they are ever effectively to tax the big tech companies.

Encryption

33. A distinct issue concerning surveillance, first raised in the crypto-wars of the 1990s, is the reluctance of internet platforms to allow law enforcement access to encrypted messages. This is not just a question of putting two fingers up to an intrusive state. The position of the companies, supported by many technical experts, is that any "back door" created for law enforcement is liable to be entered by others, fatally compromising the communications security on which we all depend.

34. The issue has become topical because of end-to-end encryption, which can make it impossible for any third party to a communication, including the service provider itself, to read the content of a message in the course of transmission. Where end-to-end encryption is in

place, law enforcement may lose all visibility of vital communications, save to the extent that they may be able to interrogate a device on which the message is stored. This affects their ability to investigate sexual exploitation and abuse, terrorism, hostile state activity and serious crime.

35. In a joint letter written to Facebook last month, the US, UK and Australian governments took issue with Facebook's plans to extend end-to-end encryption from WhatsApp to Facebook Messenger and Instagram. They made the point that this would frustrate not only their own ability to execute warrants, but *Facebook's* ability to identify and tackle the most serious illegal content and activity on its platforms. In 2018 alone, reporting from Facebook on missing and exploited children was said to have resulted in more than 2,500 arrests by UK law enforcement, and more than 3,000 children safeguarded. 70% of such reporting, it was said, would be lost.

36. In response more than 100 civil society organisations, including the Electronic Frontier Foundation, wrote their own letter to Facebook, urging it not to create "*backdoors*" or "*exceptional access*" to the content of users' messages, which they said would fundamentally weaken encryption and the security of all users. GCHQ has openly sought to initiate technical discussions with the tech companies into how real-world security could be safeguarded without prejudicing online security,[12] but there has been no public sign of a meeting of minds.

37. Facebook is not alone in asserting that its users' online privacy, and the need to preserve the integrity of strong encryption, trump even the most pressing requirements of law enforcement. Apple took a similar line in 2016 when it opposed court orders to assist, by writing

[12] Ian Levy and Crispin Robinson, "Principles for a More Informed Exceptional Access Debate", Lawfare blog, 29 November 2018.

software, in the unlocking of an iPhone belonging to one of the San Bernardino terrorist attackers.

38. No-go areas for law enforcement are in principle undesirable: and where one strongly encrypted channel already exists, the case for extending encryption to others seems weaker. Policing would surely benefit, as it does in the context of banking, from the filing of suspicious activity reports by internet platforms, and the ability when duly warranted to monitor transactions in real terms and examine stored data.

39. It might just be possible to hope that a way can be found – hopefully not prompted by a major terrorist attack – of resolving this issue by mutual consent. Should this not happen, a judicial determination could be provoked, in this country, by the service of a technical capability notice on an internet service provider under section 253 of the Investigatory Powers Act. In such a case it would be for the court to decide, on the evidence, whether the assistance required in the execution of a warrant was both reasonable and practicable, as the Act requires.

INTERMEDIARY LIABILITY / CONTENT REGULATION

40. The next issue I want to look at is the question of intermediary liability: whether, and if so how, internet service providers should be held responsible for harmful content transmitted via their platforms.

Online harms

41. The list of harms that may be facilitated by the internet is as long, if not longer, than the list of those that may be facilitated by other intermediaries such as publishers, telecoms providers or couriers. But how internet platforms should be classified, and to what extent

they should be held responsible for the content on their platforms, are vexed and unresolved questions.

42. Specific legislation covers some of the ground: we already know that eBay may be liable for trade mark infringement if it lists infringing goods on its site;[13] that there is a national cyber-security strategy (though this may require beefing up, as the Internet of Things vastly expands the attack surface of our networks) and that there are rights against data processors under the GDPR and the Data Protection Act 2018. In other respects, there are obvious and specific gaps that need to be filled: to take a topical example, the need for transparency on the sources of information produced and circulated during an election, and on the cost and sources of funding for political advertising.

43. More problematic, from the point of view of principle, is the position of intermediaries that carry criminal or simply anti-social material of the types catalogued in the Government's Online Harms White Paper of April 2019.

44. As listed in the White Paper, "*Harms with a clear definition*" include child sexual exploitation and abuse, terrorist content and activity, organised immigration crime, modern slavery, extreme pornography, revenge pornography, harassment and cyberstalking, hate crime, encouraging or assisting suicide, incitement of violence, sale of illegal good and services, underage exposure to legal content and the sexting of indecent images by under 18s. "*Harms with a less clear definition*" are said to comprise cyberbullying and trolling, extremist content and activity, coercive behaviour, intimidation, disinformation, violent content, advocacy of self-harm and promotion of Female Genital Mutilation.

[13] Case C-324/09 *L'Oreal v eBay* ECLI:EU:C:2011:474.

45. And behind that list of words is a host of complex and worrying phenomena. Under the heading "*disinformation*", for example, lurks the vast topic of what a recent report from LSE has called an information crisis, located in five "giant evils": *confusion* about what is true and whom to believe; *cynicism*: a loss of trust even in trustworthy sources; *fragmentation*: the development of parallel realities and narratives online; *irresponsibility*, because no one accepts clear responsibility for enforcing standards; and *apathy*: disengagement from society and a loss of faith in democracy.

46. Intermediaries surely have a role in minimising these harms, and some of them – whether out of public-spiritedness or a desire to protect their brand – have shown willingness to do so. But to quantify the harm done by disinformation, to attribute causation and to impose tortious liability on the carrier (or if you prefer, publisher) would be, on any view, a problematic exercise.

Critical thinking and counter-speech

47. So freedom-minded people prefer less prescriptive options: most agreeably, education in critical thinking and the offering of "*counter-speech*" in the market place of ideas where, according to John Stuart Mill and his followers in the US Supreme Court, the good may be counted upon to drive out the bad.

48. But a functioning market place of ideas depends on its participants placing the highest value on what is good and true. The phenomena of fake news and online harassment suggest that many of us prefer, on the contrary, what is sensational, bias-confirming, discriminatory and false. Research from three scholars at MIT, published in Science last year, concluded that over a 10-year period, falsehoods on Twitter travelled "*significantly farther, faster, deeper, and more broadly than the truth, in all categories of information, and in many cases by an*

order of magnitude". [14] Another recent report, from the Literacy Trust, found that only 2% of primary and secondary age children in the UK had the critical literacy skills they need to tell whether a news story is real or fake.[15] If this is the market place of ideas, it suffers from market failure.

Laws against perpetrators

49. So why not focus simply on the *originators* of harmful content? We already have laws against the dissemination of terrorist materials, malicious communication, defamation, the incitement of racial and religious hatred and the intentional causing of harassment, alarm and distress. The Law Commission is currently engaged in a project to ensure that the criminal law provides consistent and effective protection against those who commit crimes demonstrating hatred.

50. Important though it is to get these laws right, they were developed for a world of physical interactions and legal borders. They require perpetrators to be identified and brought to justice in our own jurisdictions. Those who are abroad, or who can effectively ensure their anonymity, can simply not be reached. The delicate framework of our analogue laws is not on its own sufficient to contain the turbocharged power of internet communication, let alone to discourage online behaviour that is anti-social rather than unlawful.

Self-regulation

51. What then of the intermediary platforms, and their attempts at self-regulation? Some, relating for example to child sexual images, have had a measure of success. But their inadequacy in relation for example to terrorist content is regularly exposed in Parliament, when

[14] Soroush Vosoughi, Deb Roy and Sinan Aral, "The spread of true and false news online", Science vol 359, issue 6380, pp 1146-1151, 9 March 2018.

[15] National Literacy Trust, *Commission on fake news and the teaching of critical literacy skills*, 2018.

Facebook, Twitter and YouTube are questioned by the Home Affairs Select Committee.

52. This unsatisfactory state of affairs is partly a function of the sheer size of the task, with hours of video uploaded to YouTube every second, limited numbers of human monitors and algorithms that are better at spotting nipples than spotting irony. These problems will continue whoever sets the standards. But the impression is hard to avoid that the intermediaries will respond best where they are placed under pressure.

Legal liability

53. New and specific legal liabilities may be part of the answer. The obvious template here is the German Network Enforcement Act of 2017, under which intermediaries may face fines of up to 50 million euros for failure to take down plainly illegal material within 24 hours of a complaint being received.

54. But such a strongly coercive approach could be appropriate only for the most serious online harms: and its reach is limited by the reactive, report-and-takedown model on which it is has had to be based. Article 15(1) of the e-Commerce Directive of 2000 prohibits the imposition of a general obligation on internet intermediaries to monitor or filter what people say online. Like its US equivalent,[16] Article 15 is a relic of the pre-Big Tech age of the internet. Currently under review, it still prevents, for now, the emergence of a more general duty on intermediaries to police their own platforms.

[16] Section 230 of the Communications Decency Act 1996.

Online Harms White Paper

55. Enter this April's Online Harms White Paper.[17] Taking inspiration from the Health and Safety at Work Act 1974, the White Paper proposes a duty of care on platform service operators to do what is *reasonably practicable* to protect their users from specified harms arising from the online environment that they have chosen to create. Central to the scheme is an independent regulator – perhaps Ofcom – with statutory duties to protect privacy and freedom of expression, and to pay due regard to innovation.

56. Companies will be held to account *not* for every individual item of content on their platform, but for the steps they have taken to assess the potential risk to users of their system design, and for the effectiveness of the measures they have put in place to mitigate the risk of reasonably foreseeable harm. Is uploaded material checked against child sexual exploitation databases? Are algorithms used that lead users to ever more extreme content? Are options protective of privacy made the default? Perhaps even – a currently controversial issue – what mechanisms are in place to fact-check the veracity of political messages? These are the sorts of questions that a strong regulator will be asking.

57. The regulator will consult upon codes of practice, which should be laid before Parliament. It will also constitute the enforcement mechanism, but not in the sense of sitting in judgment on particular content decisions. The regulator's focus will be *risk- based* and *systemic*: it will have powers to collect information and to issue *assessment notices* requiring operators to carry out a compliance assessment, *enforcement notices* requiring specified steps to be taken, and as a final resort, and no doubt after appropriate due process, *penalty notices* that may fine the platforms up to 4% of their

[17] *Online Harms White Paper*, CP57, April 2019.

annual worldwide turnover. The regulator will also have broader responsibilities to commission research, promote the development and adoption of safety technologies, and increase awareness of online safety and critical thinking.

58. Free speech purists recoil from imposing duties on platforms which, unlike the broadcasters already regulated by Ofcom, are still in essence conduits for private persons to communicate with one other.[18] But the imperative of free speech cuts both ways. Bullies, stalkers and foul-mouthed abusers inhibit the online freedoms of others, in much the same way as anti-social behaviour in the real world drives the most vulnerable from the public square.

59. Other criticisms of the White Paper have centred on the use of nebulous terms such as "trolling", "extremism", "harm" and "offence": terms which are certainly too broad to be treated as blanket prohibitions. Some, including the weasel word "*extremism*", could usefully be lost altogether. But "Harm and Offence" is the title of Chapter 2 of the Ofcom Broadcasting Code. And though some have feared that all-encompassing regulation will have a chilling effect on platforms, the more likely outcome is that the sheer scale of its task will require the regulator either to spread its efforts thinly or to prioritise ruthlessly. This sheriff will not tame the Wild West, but should, if all goes well, give the cattle barons something to think about.

Self-regulation

60. The White Paper scheme aims to promote effective self-regulation by the intermediaries. In that respect, the recently-released plans for Facebook's Oversight Board, the so-called "Supreme Court of

[18] See e.g. Graham Smith, "The internet: broken or about to be broken?", Keynote Speech to the SCL Annual Conference 2019, SCL blog 9 October 2019.

Facebook", are instructive. 2000 people in 88 countries were consulted on the design of the Board. Its initial 15 part-time judges, who will appoint 25 more, will hear appeals on content governance decisions, referred by Facebook's 2.5 billion users or by Facebook itself. The judges will be diverse in every possible way: no legal qualifications or experience are required. Yet the reasoned decisions of its multiple panels will need to be consistent, and of global application.

61. What Facebook describes as the "*underlying bedrock*" for the Board's decisions is yet to be decided. A recent and much-criticised speech by Mark Zuckerberg was heavily influenced by First Amendment precedent.[19] David Kaye, the UN Special Rapporteur on the freedom of opinion and expression, has counter-argued that it would be perverse to ignore the global standards that already exist in international human rights law.[20] In any event, as one lawyer put it, more than just "*a bunch of buzzwords*" is required.[21]

62. It is easy to mock the attempt. But such mechanisms, however imperfect, are conceptually exciting. They are necessary, and they are the future.

STANDARDS OF CORPORATE JUSTICE

63. The exercise of traditionally judicial functions by large multinational corporations is relevant also in relation to topics other than content regulation. Take the auction sites – the biggest of which, eBay, handles no fewer than 60 million disputes annually between its buyers and sellers. Neither the state nor a fully independent arbiter is involved at any stage: enforcement of decisions takes the form of

[19] Speech at Georgetown University, 17 October 2019.

[20] David Kaye, Report of the Special Rapporteur on the promotion and protection of the freedom of opinion and expression, A/74/48050, 9 October 2019.

[21] Thomas Kadri, quoted in Facebook's "Global Feedback & Input on the Facebook Oversight Board for Content Decisions", 2019, p. 33.

the payment of a refund or expulsion from the platform, no bailiffs necessary.

64. Cheap and convenient justice is to be applauded in principle, and even for a transaction that does not cross borders, this certainly sounds as though it beats a trip to the Small Claims Court. Detailed research is difficult, because dispute resolution algorithms are closely-guarded commercial secrets. But an article by Rory van Loo shows that while corporations may appear neutral as between buyer and seller, they want to encourage certain consumers to keep using their services: and free of regulatory constraint, their processes may be so constructed as to further this goal.[22]

65. Van Loo cites one auction platform which, as part of its automated handling of complaints, factors in:

    a. The number of past complaints, and a prediction of how the customer would react to having their complaint rejected

    b. The value of the customer to the platform, calculated on the basis of wealth, the wealth of family members and their purchasing history with a range of e-commerce companies, and

    c. The social influence of the customer, as measured by the number of Twitter followers or Facebook friends.

66. He concludes that a system which we imagine to operate impartially may "*provide less redress to consumers with smaller savings and lower-income social networks*". To put it more bluntly, it is *designed* to favour the rich and well-connected, and must therefore incorporate types of discrimination, including no doubt on grounds of

[22] Rory van Loo, "The Corporation as Courthouse" 33 Yale J. Reg. 547 (2016).

race, that the ordinary justice system, for all its faults, aims to minimise.

67. If private companies are to administer justice in that way, perhaps we need to ask whether the state should require them to conform with some basic aspects of the rule of law: and to provide transparency reports and copies of their algorithms so that their compliance can be verified.

ANTITRUST

68. My time is almost up, and you may have noticed that despite the title of this lecture series I have said almost nothing about antitrust litigation, or even competition law more generally.

69. There are, indeed, a series of fascinating conceptual issues relating to antitrust law and its application to big tech.

    a. Whether US antitrust law needs to throw off the Borkian shackles of consumer welfare analysis.[23]

    b. How dominance is to be assessed, and its abuses mitigated, in industries whose principal value lies in data.

    c. Whether services that appear to be provided for free are nonetheless excessively priced because of the value of the data that is extracted from their users.

    d. How far it is legitimate for competition law to be used to enforce data privacy concerns, as in the German Facebook decision, or indeed other societal goals such as algorithmic transparency.

[23] See Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, Random House, 2018.

e. Whether as floated in the EU it is feasible to impose upon large internet companies the burden of proving that their conduct benefits consumers, forcing them to disgorge the relevant data.[24]

f. Whether, in the delicate phrase of our Digital Competition Expert Panel, it is wise to "*adjust appeal standards*" in the CAT.[25]

g. Whether big tech companies should be broken up, for example by separating platform utilities from participants on that platform, as promoted by the Democratic candidate Elizabeth Warren.

h. Whether merger control needs to get better at preventing the early elimination of small potential rivals, and advance beyond the procedural infringements of the kind so severely punished in the Facebook/Whatsapp merger.

i. And finally, whether that distinctively UK mechanism, the Enterprise Act market investigation, might be usefully deployed.[26]

70. So fascinating are such questions that they almost make me wish I had stuck with competition law. But I decided against trying to answer them today for two reasons: first, the wise advice of Wittgenstein to stay silent about that on which one cannot speak, and secondly the hope that if I did keep quiet, a future and better qualified Vaughan Lecturer may be counted upon to address them with the care and the expertise that they deserve.

71. I look forward to being there on that occasion.

Thank you.

---

[24] Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, "Competition policy for the digital era" (EU Commission, 2019).

[25] "Unlocking digital competition", Report of the Digital Competition Expert Panel, March 2019.

[26] As suggested by Sir Peter Roth in his Blackstone Lecture "The Continual Evolution of Competition Law", 9 November 2018.