Three wise monkeys of net neutrality: privacy, liability and interception

DPI can look into the content of the message sent over the Internet. To use a real-world example, using DPI is akin to a third party opening an envelope sent by surface mail, and reading its contents before it reaches its intended destination … it is not clear that examination of content is necessary for network management and may constitute an unreasonable invasion of an individual’s privacy.

Privacy Commissioner of Canada¹

IAPs have been acting as the fabled ‘three wise monkeys’ in relation to Internet content liability since the dawn of the commercial Internet.² These intermediaries are not subject to liability for their European customers’ content under the Electronic Commerce Directive (EC/2000/31) (ECD) so long as they have no actual or constructive knowledge of that content: if they ‘hear no evil, see no evil and speak no evil.’³ Regulators have also been acting as ‘three wise monkeys’ in ignoring evidence that net neutrality is being compromised by IAP decisions to block, throttle and otherwise censor users’ access to content. Forms of private censorship by intermediaries have been increasing throughout the twenty-first century even as the law continues to declare those intermediaries (mainly IAPs, but increasingly also video-hosting companies such as YouTube, social networks such as Facebook and search providers such as Google) to be ‘Three Wise Monkeys’. The liability question may be paraphrased: will the

¹ Privacy Commissioner of Canada (2013b) at paras 13, 32.
monkeys continue to be wise conduits for speech, or will governments make them open their eyes and ears, becoming censors of speech and recorders of our every click online?

Governments have been fundamentally challenged in both the European Union and the United States by the Snowden revelations of mass surveillance. Much of this surveillance took place with the secret cooperation of the IAPs, as required by the conditions of their permissions to conduct their business. This chapter is an empirical examination of the use of interception by IAPs, whether required by law enforcement or for the IAP’s own purposes, such as for behavioural advertising. It does not consider the wider theoretical foundations of electronic privacy, the wider implications of Snowden’s revelations for providers other than IAPs, or the specific legal reforms imposed in response to the potential illegality of state surveillance under programmes such as Tempora. I do not consider in this chapter the wider implications of the cases that led to the annulment of the Data Retention Directive (2006/24/EC)6 in 2014, nor the US–EU Safe Harbor in 20157 and its putative replacement, the Privacy Shield, announced in February 2016. The General Data Protection Regulation (GDPR) was also confirmed in 2016.8 Books and articles will be written about such issues in the coming months and years, and the net neutrality blog (chrismarsden.blogspot.com) will refer to them as privacy developments become clearer. Books and articles will continue to be written about various national laws retrospectively securing the legality of surveillance, such as the UK Investigatory Powers Bill 2016, which was proceeding through Parliament as I wrote this book. The so-called Right to be Forgotten (or obscure) is also a topic for other scholars.9 I focus on the IAP legal regime for net neutrality, the surveillance requirements that may infringe net neutrality, and finally the extraordinary cases of behavioural advertising without the permission of users that were carried out by BT, and which resulted in legal action against the UK government for inadequate enforcement of European privacy legislation, namely the E-Privacy Directive 2002/58/EC.10

5 Joined cases C-293/12, Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and C-594/12 Kärntner Landesregierung and Others.
7 C-362/14, Maximillian Schrems v. Data Protection Commissioner, Judgment of Grand Chamber 6 October 2015.
9 C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González; Powles (2015).
It is important that governments consider where best the issue is regulated, by a telecoms regulator or by a ministry. The net neutrality privacy problem is not a lack of regulatory tools per se, but potentially a lack of forensic skills to analyse the potential consumer harms that can be created by unjustified or ‘unreasonable’ discrimination. Regulators can monitor both commercial transactions and traffic shaping by IAPs to detect potentially abusive discrimination. No matter what theoretical legal powers may exist, their usage in practice and forensic gathering of evidence may make the regulatory task very burdensome. The increasing use of behavioural advertising by third parties is also very concerning to privacy regulators, and any cooperation between IAPs and third parties to share such revenue is likely to need the explicit consent of all IAP users, following the precedent of the Phorm case considered below, and European opinions recently issued about behavioural advertisers.¹¹

First, I place interception in the regulatory context, to explore neutrality as a form of ‘medium law’ as well as the policy implications of the Snowden leaks and other recent developments. Second, I analyse the legal, technical, regulatory and policy discussions that have been applied to this form of interception. I discuss global problems that private or ‘co-regulated’ filtering and censorship cause, whether for private ends, such as copyright enforcement, or public ends, such as restricting freedom of expression, as well as the potential impact on developing countries. The major part of the chapter deals with the BT and Phorm experiments of 2006–08, the UK government’s encouragement of such illegal activities and the European Commission’s responses that forced amendment to UK e-privacy law in 2012. Finally, I assess the evidence base for future privacy legislation affecting IAPs, the EC ‘Platform Regulation’ consultation, and the need for regulators to address privacy in net neutrality policy discussion in future.

The GDPR and the Snowden inquiries 2016

European laws are meant to protect citizens’ privacy and liberty. Directive 95/46/EC is the main law giving responsibilities to Member States and data protection rights against corporate actors to citizens. This European law sets a high standard for data protection, arguably higher than that in the United States. National data protection agencies have a permanent joint working group (the Article 29 Working Party) and are required to implement the Directive as uniformly as possible; its tasks include members cooperating with each other and

the European Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to a high level of protection of personal data and privacy, and ensuring that the integrity and security of public communications networks are maintained.\textsuperscript{12} The European institutions are also required by law to consider the Opinions issued on prospective legislation by the EDPS, established in 2002. Directive 2002/58/EC (the ‘E-Privacy Directive’) includes measures intended to prevent spam, which are supplemented by a 2004 Communication\textsuperscript{13} on spam.\textsuperscript{14} The critical test in both Directive 2002/58/EC and Directive 95/46/EC is that subscribers have to opt for arrangements that may otherwise infringe their personal privacy, and that sensitive data must not be passed to third parties unless so authorised by subscribers and the data is anonymised.

The GDPR amends the E-Privacy Directive and replaces and repeals the Data Protection Directive (DPD).\textsuperscript{15} The draft Regulation COM(2012) 11 in particular contained Sections 42–43 relating to transfer of data outside the European Union, insisting on Binding Corporate Rules (BCR) for such transfers to take place subject to enforcement by national data protection agencies (DPAs).\textsuperscript{16}

One area in which European regulators have been forced to investigate potential interception, very much against net neutrality principles, is that of illegal surveillance of IAP users perpetrated by agencies in the ‘Five Eyes’ multinational espionage coalition.\textsuperscript{17} Note that though nation-states funded these activities, they were carried out with the more or less willing cooperation of Internet companies including IAPs acting against their own users’ interests in net neutrality. Illegal as well as legal interception activity by ‘Five Eyes’ within European, Latin American and other nations was exposed by the whistle-blower Edward Snowden and The Guardian newspaper in June to October 2013.\textsuperscript{18} ‘Five Eyes’ (or more formally AUSCANNZUKUS) describes the cooperation between the intelligence (i.e. espionage) agencies of the Anglo-Saxon powers during what in English-speaking countries was called the Cold War between the US/allies and the Warsaw Pact/allies.\textsuperscript{19} The United States, United

\textsuperscript{13} Communications from the Commission, and Resolutions of the Council are not European legislation and therefore non-binding on Member States, but they have important ‘signaling’ effects on Member States and companies and therefore are termed ‘soft law’.
\textsuperscript{16} COM(2012) 11 and COM(2012) 09. See also IP/12/46.
\textsuperscript{17} Campbell (1999).
\textsuperscript{18} Bowden (2013a).
\textsuperscript{19} Richelson and Ball (1985).
Three wise monkeys of net neutrality

Kingdom, Canada, Australia and New Zealand are formal partners, though other allies have subsidiary and subsequent agreements that permit some level of intelligence sharing.20

Packet-snooping schemes such as Carnivore, a system implemented by the Federal Bureau of Investigation that was designed to monitor email and electronic communication, have been active since at least 1997; Carnivore had used a customisable packet sniffer that can monitor all of a target user’s Internet traffic.21 A larger-scale operation, called Echelon, was built by various Western governments, and this was investigated by the European Parliament in a report released on 5 September 2001.22 Surveillance by Intelligence agencies has vastly increased, as exposed thoroughly by Glenn Greenwald and colleagues at The Guardian using evidence supplied by former National Security Agency contractor Edward Snowden.23 Echelon was later replaced by the US programme PRISM24 and in 2011 UK–US joint operation Tempora (with sub-programmes called ‘Mastering the Internet’ and ‘Global Telecoms Exploitation’), which intercept communications in fibre optic cables destined for transatlantic transmission.25 Law in this area is rapidly outflanked by the technological capabilities of public and private parties, which has resulted in inquiries in response to the Snowden revelations, notably by the Intelligence and Security Committee:

> Although we have concluded that GCHQ has not circumvented or attempted to circumvent UK law … We are examining the complex interaction between the Intelligence Services Act, the Human Rights Act and the Regulation of Investigatory Powers Act, and the policies and procedures that underpin them, further. We note that the Interception of Communications Commissioner is also considering this issue.26

This press release absolved GCHQ of any illegality, but a proper inquiry led by the Deputy Prime Minister followed in winter 2014. The Interception of Communications Commissioner (ICC) submits Annual Reports to the Prime Minister in the summer after the conclusion of the previous calendar year.27 Despite the urgency of the public revelations of the potentially illegal use of Tempora programmes by GCHQ in June 2013, the ICC announced that he

---

20 The initial formal UK–US agreement was signed in 1947 after the successful conclusion of the Second World War and just prior to the outbreak of the Korean War of 1950–53, with final partner New Zealand joining only in 1980. See AUSCANNZUKUS (2013).
21 For a legal perspective on private packet sniffing, see Frieden (2008).
23 For examples, see Borger (2013).
24 Government code name for a data-collection effort known officially by the SIGAD US-984XN.
27 House of Commons 571 SG/2013/131.
would submit the investigation into the GCHQ interception of communications to the Prime Minister in July 2014:

[ICC] is required by section 58(4) of RIPA [Regulation of Investigatory Powers Act 2000] to report annually to the Prime Minister. The Prime Minister lays the report before Parliament except for any sensitive parts of it which he decides to exclude under section 58(7). 28

He further explained that:

my role is defined in Section 57(2) of RIPA. I am not appointed or authorised to oversee all of the activities of the intelligence agencies, only those specified in Section 57(2) of RIPA. I can confirm that I am currently conducting an investigation into the various recent media reports relating to disclosures about interception attributed to Edward Snowden. 29

Much of the relevant intercepted data is metadata, which is more useful to intelligence services and behavioural advertisers than is content of communications, which is not machine-readable and therefore examining it in large volumes would be too time-intensive to be useful. Part I Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) covers the acquisition and disclosure of communications data (rather than the content of the communications). Therefore, some element of scrutiny of public authorities’ use of metadata commenced and was reported internally in July 2015. Metadata was also a key concern of the Article 29 Working Party in its study of the reform of European e-privacy law. 30

The Snowden revelations allege illegal interception of IAP traffic, which supports earlier European Parliament investigations, and has brought complaints about violations of criminal law to the attention of the European human rights court, national parliaments and information commissioners. 31 The interception laws of most nation states do not permit IAPs to allow or condone interception by third parties, let alone foreign state agencies. Brown provides a useful summary of such laws in several states, including the ‘Five Eyes’ signatories themselves. 32

Note that the personal data of EU citizens captured by non-EU countries is still subject to European law under the 1995 and 2002 legislation until the new GDPR comes into effect in 2018. 33 In 2016 there were profound investigations

28 Interception of Communications Commissioner (2013).
29 Part I Chapter 1 of RIPA provides the statutory authority for the lawful interception that takes place within the UK.
31 Brown (2013a).
32 Brown (2013b).
33 Rauhofer and Bowden (2013).
Three wise monkeys of net neutrality

into the invasion of user traffic streams throughout Europe, with investigations in the United Kingdom, Netherlands, Belgium, France, Germany, Luxembourg and many other nations, as well as investigations by the European Parliament. Focus is on foreign spying, but as details emerge of the interception techniques used, more attention is being focused on the specific national criminal violations by agents acting on behalf of ‘Five Eyes’, notably IAPs.

While this type of interception is not classified as net neutrality violation, given that it is carried out under the orders of government and is thus presumed to be for law enforcement, should it be proven unlawful, it will amount to interception of user personal data for illegal purposes. Regulators may therefore need to issue instructions to IAPs and others not to cooperate with foreign state agencies and others who instruct them to cooperate with data gathering. In extreme circumstances, that could potentially require IAPs not to interconnect with US- and UK-based IAPs. The OECD has also renewed its privacy guidelines, and referred to the need to ensure that Internet policy conforms to fundamental rights of users. At the 2011 Paris meeting in which the latter declaration was made, the Korean delegation requested that the OECD pay attention to the need for more research and coordinated policy towards net neutrality.

What is changing in IAP analysis of traffic?

IAPs have many reasons to manage traffic:

1. It is required for government law enforcement and security purposes.
2. Network providers already provide filters against the more obvious types of ‘spam’ – unsolicited commercial communications.
3. Network providers cooperate with national security agencies in tracing potential terrorist activities on the Internet.
4. Network providers can trace non-encrypted VoIP (e.g. Skype) and block these packets.
5. Network providers are increasingly adopting Specialised Services for their networks in order to prevent users from overstraining the network at times of peak usage, and charge content owners for value-added high-volume services such as video files.

These new policies allow network providers to block file transfers, or to charge the users a carriage fee for sending large files. This policy is generally termed a

---

34 Agence France-Presse (2013).
36 See generally Bendrath (2009).
'walled garden' to denote the isolation of content on the network from other content on the wider Internet.

IAP routers (if so equipped) can look inside a data packet to 'see' its content, via DPI. Less powerful routers conduct only shallow inspection that simply establishes the header information – the equivalent of the postal address for the packet. An IAP can use DPI to determine whether a data packet values high-speed transport – as a television stream does in requiring a dedicated broadcast channel – and therefore offer higher-speed dedicated capacity to that content, typically real-time dependent content such as television, movies or telephone calls using VoIP. Most voice calls and video use a dedicated line, a copper telephone line or cable line: they may use SpS in future. That could make a good business for IAPs that wish to offer higher capability via DPI. Not all IAPs will do so, and it is quite possible to manage traffic less obtrusively by using the DiffServ protocol to prioritise traffic streams within the same Internet channel.

IAPs are using 'black boxes' in their networks to look inside the packets that carry communications and to examine their content, in a change to DPI which has very serious regulatory implications. DPI and other techniques that let IAPs prioritise content also allow them to slow down other content, as well as speed up content for those that pay (and for emergency communications and other 'good' packets). Encryption is common in applications and partially successful in overcoming these IAP controls, but even if all users and applications used strong encryption, this would not succeed in overcoming decisions by IAPs simply to route known premium traffic to a ‘faster lane’, consigning all other traffic to a slower, non-priority lane (a policy explanation simplifying a complex engineering decision).

Waclawsky stated in regard to MPLS, a mobile industry protocol to permit QoS: ‘This is the emerging, consensus view: [it] will let broadband industry vendors and operators put a control layer and a cash register over the Internet and creatively charge for it.’ Putting a cash register on the Internet will permit much more granular knowledge of what an IAP’s customers are downloading and uploading on the Internet. That means that the formerly ‘Wise Monkey’ IAPs would rapidly become the all-seeing eye, with many more consequences than simply a new revenue stream to build higher-speed lanes – which generally means laying fibre optic cables closer to the household, replacing the old copper lines. IAPs could filter out both annoying and illegal content. For instance, they could ‘hear’ criminal conversations, such as those between terrorist sympathisers, illegal pornographers, harassers, those planning robberies, those containing libellous commentary, and so on. They could also ‘see’ illegal downloading of copyrighted material. They would be obliged to ‘speak’, to cooperate with law enforcement or even copyright industries in these scenarios,

and this could create even greater difficulties where that speech was legal in one country but illegal where it was received. Examples include English libel law, Australian pornography filtering, Chinese Falun Gong website blocking, Turkish YouTube bans and United States online gambling bans. Net neutrality is therefore less unpopular with smaller IAPs that wish to avoid a legal liability morass, which the E-Commerce Directive and other national IAP non-liability ‘safe harbor’ laws are expressly designed to prevent.

IAP (and government) practices have been highly deceptive in places, blocking content for specific anti-competitive and non-specific traffic management purposes. Attempts at least to introduce transparency into the debate, as well as the rights of end users, can be achieved via co-regulation. In European telcos, this is a prevalent but awkward compromise between state and private regulation, with constitutionally uncertain protection for end users and wide latitude for private censorship.

Mobile IAPs claim the same special protections from regulation that their previous incarnations as mobile voice networks claimed, to enable walled gardens to flourish. It is worth noting that many mobile IAPs use IMSI and other parsing methods to track everything users do on the Internet, in developed and developing countries, with increasing levels of technical sophistication. Any net neutrality solution needs to be holistic, considering IAPs’ roles in the round. IAPs are a heterogeneous category, ranging from very large network owners such as (UK examples) British Telecom, Vodafone and Virgin Media (owner of the cable TV/telecoms infrastructure), to large retailers such as TalkTalk and Sky, to hundreds if not thousands of much smaller niche business and consumer operators. Smaller operators do not typically deploy such widespread interception capability, with the most privacy-aware, Andrews & Arnold Ltd, stating: ‘We have no so called black boxes to covertly monitor traffic and/or pass traffic monitoring to the authorities or anyone else. Obviously the law is such that we may have to add such black boxes, but we would resist as far as possible.’ Other IAPs are not so protective of their users’ privacy.

DPI is a technique that may be both unreasonable and invasive of user privacy, and it may be that information/privacy commissioners are best placed to investigate such potentially criminal breaches of user rights. Because net neutrality raises a set of new issues for privacy regulators, the necessary skill set needs to be acquired and developed in consultation with other national and international regulators. Currently, it is not a requirement for most IAPs to

---

38 International Mobile Subscriber Identity (IMSI) identifies a cellular network user, and is stored as a 64-bit field on the SIM card.

39 Vallina-Rodriguez with Sundaresan, Kreibich and Paxson (2015). The paper describes privacy violations and header enrichment practices performed by mobile operators (perma-cookies, x-forwarded-for, IMEI, IMSI, etc.).

notify customers when they block encrypted content, such as P2P-distributed applications. The (often spurious) security or anti-piracy reasons given are not within the remit of typical economic telecoms regulators. Where the reasons given by some IAPs for blocking encrypted traffic, which carries malware and other harmful content, are typically the concern of the security services (Interior Ministry or Prime Minister’s office), and occasionally the Ministry of Industry, the regulator defers to these senior agencies because it has little technically specific knowledge of data security.41 More joined-up regulation is needed with urgency in this field. Regulators and politicians are challenged publicly by such problems, particularly given the ubiquity of email, Twitter and social media protests against censorship.

Network neutrality cannot simply be solved by economic analysis of bottlenecks in transport-based industry, or a convergence of regulation between television and the Internet, but as the delivery mechanism for the global Information Society. The Internet’s core values of openness and democracy have been established by accident as well as design. ‘Medium law’ (i.e. mass market content online that formerly used several media) is intimately tied into telecoms law. Security and antiterrorist measures are also driving IAPs towards filtering all incoming traffic. This may change the entire architecture of the Internet, its business model and freedom of speech. It is happening beyond the analysis of the discrete fields of information security, e-commerce law, media law and telecoms law.

There are at least two critical non-IAP-originated factors at play: concern over illegal and inappropriate content (such as child pornography, music protected by copyright and latterly video files being inappropriately shared, and malware including spam); and the security agenda, which aims to enforce QoS to separate ‘good’ or preferred from ‘bad’ or discriminated-against packets. There is a legitimate concern that this represents a division between the rich and powerful senders of packets and the lesser content types. These three policy areas – telecoms, content and security regulation – are coming together. Horten states:

By authorizing blocking practices, the Telecoms Package puts Europe on a path to a closed series of Internets. It puts at risk innovation, trade, and any policy goals to encourage cross-border trade. It puts at risk the EU’s Information Society goals. And, it stands to chill democratic speech.42

The problems of development and the global Digital Divide are intimately connected to net neutrality. Internet connectivity is still very expensive for most developing countries, despite attempts to ensure local Internet peering points

42 Horton (2009).
(exchanges) and new undersea cables, for instance serving East Africa. Mobile access is considered further in Chapter 7. Mueller argued that net neutrality ‘must also encompass a positive assertion of the broader social, economic and political value of universal and non-discriminatory access to Internet resources among those connected to the Internet’. He also argued that the tendency of governments in both repressive and traditionally democratic regimes to impose liability on IAPs to censor content for a plethora of reasons argues for a policy of robust non-interference:

The flip side of a [network neutrality] policy that valorises the right of Internet users to access each other without interference from intermediaries is the belief that network users wronged by other users must hold the wrongdoer responsible – not the intermediary network operator.

That is especially valuable in countries where there is much less discussion of how government deployment of IAPs as censors can endanger user privacy and freedom of expression. Mueller suggested that the net neutrality metaphor could be used to hold all filtering and censorship practices up to the light, as well as other areas of Internet regulation, such as domain name governance. Network neutrality has become an important policy issue that is discussed at the United Nations Internet Governance Forum (IGF). The IGF discussions of net neutrality and other issues substantially increased from 2009 to 2015, as explored in Chapter 8.

Law and technologies to intercept communications

Committees of both the US Congress and the UK Parliament carried out inquiries into behavioural advertising in 2009. Since 2002, Article 15 ECD has also required European Member States not to impose undue restrictions on IAPs, which continually causes Member States to either derogate from the ECD in the interests of crime fighting and anti-terrorism law or simply

---

44 Ibid., p. 8.
46 Directive 2000/31/EC, Article 15 states: ‘No general obligation to monitor. 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transit or store, nor a general obligation actively to seek facts or circumstances, indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements’.
to ignore the provision altogether. So many features of wire tapping and anti-terrorism law have been passed or amended since 2001 that there would by now be several thousand derogations across the European Member States, given that interception of communications by IAPs on behalf of governments formally requires a notification for derogation from Article 15 for each of the 28 Member States whenever anti-terrorist law is reformed in this area. The definition of the limits on general obligations to monitor – which are relevant for any imposition of, for instance, copyright monitoring on IAPs by Member States – were explained by the European Court of Justice in the 2012 leading case of SABAM v. Netlog NV. The Court held that imposing a copyright-filtering system on an IAP would infringe on the prohibition on general obligation to monitor, and stated that it:

[Para. 48] may also infringe the fundamental rights of that hosting service provider’s service users, namely their right to protection of their personal data and their freedom to receive or impart information … [Para. 49] Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users [protected personal data].

Note that the proposed reforms of the ECD including Article 15 were abandoned in 2012 by the European Commission in its E-Europe Action Plan. It is well established that no governmental authority or court can impose a general duty to intercept and monitor, because that would infringe privacy rights.

The range of network and information security requirements at European level, which must then be implemented as national law in the European countries, imposes costs on the network. These are in addition to existing costs for spam filtering, protection against distributed denial of service (DDOS) attacks, phishing and other ‘malware’ that IAPs typically invest in to protect their subscribers from the worst excesses of IP traffic. Security is a growing problem as dependence on broadband (as a key element of the critical information infrastructure) grows and as the Internet moves towards pervasive computing, and the ‘Internet of Things’. There is an escalating arms race as criminal behaviour becomes more sophisticated. The objectives and requirements are also changing on both sides: on the attacking side, the evolution from unauthorised access to data corruption, exposure or access denial; on the defending side, the change in data collection, storage, processing locations (centralised or not), data exchange and transfer of liability among buyers, sellers and IAPs. Loss of Internet privacy, openness and E2E connectivity is one potential casualty of security concerns.

47 Case C-360/10, Reference for a preliminary ruling under Article 267 TFEU from the rechtbank van eerste aanleg te Brussel (Belgium).
IAPs can either throttle users by cutting off their connections at peak times, once they have exceeded monthly quotas, or try looking inside the packets to see whether they are P2P or not. The latter becomes a very dangerous business to engage in because, as we will see, governments are not only encouraging IAPs to look, they are actually subsidising the DPI equipment required to do so – and this sometimes in breach of both European and UK privacy and interception laws (the latter intended to prevent private spying, even if encouraged by government policy). Felten worried that regulators are used to standard bodies and classes of companies, when, for instance, BitTorrent is a protocol, not a company or a single standard. Blocking BitTorrent or P2P more widely will eventually fail because the protocol designers will route around via encryption or other techniques.

Regulating DPI and interception of traffic

Blocking and other forms of traffic shaping are controversial because, under current network management tools, they are blunt tools. For instance, all P2P traffic using a certain protocol may be blocked. P2P can respond by encrypting its traffic or otherwise spoofing, but this creates an ‘arms race’ much like that found in security software responses to the threat of breaches. Future networks may try to cap P2P more effectively, which can itself lead to an ‘arms race’ between encrypted P2P content and attempts by IAPs to detect P2P traffic using DPI.

IAPs have limited liability where they act as ‘mere conduits’ but not where they have constructive or actual knowledge of illegal content. Their traffic is thus something of a Pandora’s box – if they look inside using DPI, all liabilities flow to them, from child pornography, to terrorism, to copyright breaches, to libel, to privacy breaches.

Cooper analysed the choices of whether to introduce DPI equipment into IAP networks, restricting traffic as an alternative to increasing capacity, with the consequent decision to invest in DPI and other management servers instead of greater bandwidth. She points out that US cable companies at the time of the Internet Policy Statement in 2005 hoped that the burden of proof on ‘reasonable’ techniques would fall on complainants, with the presumption that

48 Felten (2008).
49 In May 2009, uTorrent announced a future protocol change to UDP, which indicates that (a) TCP may not be the main P2P traffic protocol; (b) that will annoy those who use TCP for YouTube etc.; (c) it will annoy ISPs; (d) so more discriminatory actions can be expected. It is the arms race continuing at a higher level, as filtering UDP is a new departure for many consumer ISPs. See www.theregister.co.uk/2008/12/01/richard_bennett_utorrent_udp/ (Accessed 5 September 2016).
50 Cooper (2013), pp. 109–120.
IAPs were acting reasonably. That has not been the case in the US or Canada. It is for the IAP to demonstrate that its use of technologies such as DPI is reasonable, a test that Comcast failed in its deployment of Sandvine DPI. The presumption that DPI may be unreasonable based on Comcast’s experience has been profound for US IAPs. Cooper concluded that while marketing directors still encouraged DPI use and were likely to authorise such expenditure in order to better target services at customers, regulatory departments discouraged its use and had the reverse effect on which engineering choices to deploy. More research is needed into the causes for such differences, but it is very likely that a lack of knowledge and education about the criminal offences from breaching data protection law and intercepting traffic amongst marketing departments of IAPs may account in part for their cavalier approach to installing DPI equipment to monitor customers. By contrast, engineers’ typical preference in Cooper’s study was to increase bandwidth rather than manage traffic more minutely.

It is also notable from Cooper’s study that foreign content providers were unable to influence domestic IAPs’ traffic management practices, so that MMORPG (massively multiplayer online role playing game) providers such as World of Warcraft were often significantly impeded in delivering their service because of unreasonable traffic management, a problem significantly worse in the UK where DPI and other traffic management techniques were used much more invasively than in the US. Cooper’s conclusions have particularly negative outcomes for those free-to-play MMORPGs such as are commonly found in South Korea, as there would be no likelihood that such MMORPG creators could negotiate or even complain successfully when foreign IAPs block their world.

Cooper establishes that different countries’ regulators view of litigation and reputation is likely to colour their view of what is ‘reasonable’ and how strict their interpretation of that provision may be. Thus the US regulators are not scared of litigation or enforcement and so are likely to prosecute cases more strictly, whereas the lawyer-light UK regulator is committed to alternatives to enforcement and is likely to prosecute only as a last resort. UK regulators, notably the Information Commissioner, have shown no willingness to prosecute even in the infamous case of PHORM/BT’s illegal DPI trial, whereas the US regulator Federal Trade Commission (FTC) successfully brought strict settlements with multimillion-dollar fines for social networks that misused their subscribers’ data, notably Google and Facebook in August 2012. In the Google case, the FTC declared its first:

52 Cooper (2013), pp. 122–132. Cooper interviewed 70 elite decision-makers in ISPs, regulators and content companies in the period 2011–12, the broadest sample known.
53 Ibid., pp. 200–204.
55 Lardinois (2012).
FTC settlement order [that] has required a company to implement a comprehensive privacy program to protect the privacy of consumers' information. In addition, this is the first time the FTC has alleged violations of the substantive privacy requirements of the U.S.–EU Safe Harbor Framework.  

The likelihood of criminal or civil prosecution for breaches of net neutrality and other abuses of trust with IAP users are thus conditioned by the regulators' willingness to actually enforce regulation. In the US this is clearly the case; in Europe very much less so. This is despite the US corporate need to satisfy European regulators that the theoretically weaker US personal data privacy rules can satisfy European law under existing Directive 95/46/EC. As has become apparent in the wake of the 2013 Snowden revelations, US companies are both constantly in breach of the safe harbour themselves for corporate policy reasons, and obliged by US law enforcement and espionage to mistreat personal data of citizens of other countries, including Europeans and Koreans. Belatedly, this became a significant issue in the renegotiation of the ‘Safe Harbor’ and the GDPR in 2016.

Alleged criminal breaches of UK e-privacy by IAPs

The continued attempts by IAPs to intercept communications on their own networks are by themselves legal under the law of interception. However, they may not allow others to intercept on their behalf or grant to others the right to intercept for their own purposes. UK law is clear on this point. Interception of communication is subject to RIPA Section 2(2):

For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he –

(a) so modifies or interferes with the system, or its operation,  
(b) so monitors transmissions made by means of the system, or  
(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

One element of intercepting is that making available some or all of the contents of the communication to a person other than the sender or intended recipient

57 FTC (2011).  
58 European Commission, Consultation on the Commission’s comprehensive approach on personal data protection in the European Union, 4 November 2012.
is not permitted. Whether or not some of these contents (via the channels) are made available to anyone other than the IAP or a third party, they are available to someone other than the sender/recipient. The UK test is strict and requires both parties (sender and receiver) to consent.

The most controversial of all attempts by UK network owners to intercept users’ communications without consent were the experiments conducted by the behavioural advertising company Phorm with the UK’s largest IAP BT (and discussions with the next two largest, TalkTalk and Virgin Media\(^{59}\)). Phorm employs a user-tracking system by which British Telecom and other IAPs intended to target users more effectively than Google. A variant of this technology was first deployed widely in US wireless IAPs.\(^{60}\) Phorm operated a behavioural advertising system called WebWise, intending to offer its IAP and website clients a more accurate tracking of customers’ Internet use, in order to more closely target advertising and other marketing via that data.

Phorm used DPI to take a copy of IAP subscribers’ Web browsing, in order to insert targeted advertising. The original Phorm system trials by BT in 2006 and 2007 did not inform users or ask for their permission.\(^{61}\) The government department responsible for interception of electronic communications was aware of, and tried to provide helpful regulatory guidance on, the trials and the behavioural advertising system. It emerged in April 2009 that the department, when contacted by Phorm in August 2007, had responded by asking ‘If we agree this, and this becomes our position, do you think your clients and their prospective partners will be comforted?’\(^{62}\) It appears that the consultations between the department and Phorm were extensive and amounted to forming a collaborative view of the law, with comments such as ‘My personal view accords with yours, that even if it is “interception”, which I am doubtful of, it is lawfully authorized under section 3 by virtue of the user’s consent obtained in signing up to the IAPs’ terms and conditions.’\(^{63}\) In an email dated 22 January 2008, a Home Office official wrote again to Phorm and said: ‘I should be grateful if you would review the attached document, and let me know what you think.’\(^{64}\) The publication of this history of emails resulted in a debate in the House of Lords in 2009. Baroness Miller stated that:

\(^{59}\) Williams (2009c).


\(^{61}\) Dubious value is given to such permission in BT internal documents, see http://wikileaks.org/wiki/British_Telecom_Phorm_PageSense_External_Validation_report (Accessed 5 September 2016).

\(^{62}\) BBC (2009).

\(^{63}\) Marsden (2010), p. 79.

\(^{64}\) Ibid.
Three wise monkeys of net neutrality

The fact the Home Office asks the very company they are worried is actually falling outside the laws whether the draft interpretation of the law is correct is completely bizarre.\(^65\)

As a result of the legal controversy that followed when the trials were made public in early 2008, the IAPs and Phorm itself agreed to insert both notification and consent into any future trial or deployment of the technology, and BT did so for its third trial in December 2008. In legal terms, the system is not just contrary to permissions required in European privacy law under the 1995 and 2002 Directives, but also unlawful interception under the exclusively UK RIPA. In March 2008 the Foundation for Information Policy Research (FIPR) wrote to the Information Commissioner arguing that Phorm’s system involved illegal interception contrary to RIPA.\(^66\) Citizens’ complaints about the use of behavioural advertising by Internet service providers were handled by the UK Information Commissioner’s Office (ICO), the UK personal data protection authority and the police forces responsible for investigating cases of unlawful interception of communications. All had failed to adequately investigate the criminal complaints, in part due to the ICO’s weak powers to fine aberrant providers. The UK’s Information Commissioner ruled that a ‘technical’ breach of the law occurred in BT’s 2006–2007 trials, and had strong reservations about the nature of the explanation provided for participating in BT’s 2008 trial, but took no action.

Clayton, a security expert at Cambridge University, presented a report on the system, to which Phorm responded to ensure technical accuracy.\(^67\) Clayton stated: ‘Examining the detail makes it crystal clear that our earlier letter came to the right conclusion. Website data is being intercepted. The law of the land forbids this.’\(^68\) The illegality stems not from breaching the Data Protection Act directly, but arises from the fact that the system intercepts Internet traffic. BT appeared to ignore the fact that they can only legalise their activity by getting express permission not just from their customers, but also from the Web hosts whose pages they intercept, and from the third parties who communicate with their customers through Web-based email, forums or social networking sites.

The EC takes the UK to court for net neutrality privacy breach prosecution

In response to UK citizens’ complaints that the ICO was failing to prosecute Phorm and BT for breaching the 1995 Directive in not asking consent for the

---

\(^{65}\) LINX Public Affairs (2009).

\(^{66}\) See FIPR (2008).

\(^{67}\) Clayton (2008).

\(^{68}\) FIPR (2008).
original trial, the European Commission formally asked the UK government to explain why action had not been taken. The European Commission is tasked with monitoring Member States’ implementation of European law, in this case Directive 2002/58/EC, the Electronic Privacy Directive (EPD). The Data Protection Directive (DPD) of 1995 specifies that user consent must be ‘freely given, specific and informed’, a formula repeated in the EPD. The critical test in both the EPD and the DPD is that subscribers have to opt for arrangements that may otherwise infringe their personal privacy, and that sensitive data must not be passed to third parties unless so authorised by subscribers and the data is anonymised. The EPD requires EU Member States to ensure confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented to this. Article 24 DPD requires Member States to establish appropriate sanctions in case of infringements. Article 28 requires that independent authorities must be charged with supervising implementation. These DPD provisions also apply to confidentiality of communications.

When the UK response received was unsatisfactory, the EC repeated its request for information in stronger terms. When that second response was unsatisfactory, in January 2009 the Commission threatened legal action and launched legal action in an infringement procedure against the UK in April 2009. Commissioner Reding declared:

I call on the UK authorities to change their national laws … This should allow the UK to respond more vigorously to new challenges to ePrivacy and personal data protection such as those that have arisen in the Phorm case.

In October 2009 the Commission requested the UK authorities to amend their rules to comply with EU law, due to inadequate national legal implementation in three main areas:

- There was no independent national authority to supervise the interception of some communications, although the establishment of such authority is required under EPD and DPD, in particular to hear complaints regarding interception of communications;
- Existing UK law allowed the interception of communications not only where the relevant internet users have consented to this but also where the person intercepting the communications has ‘reasonable grounds for believing’ the

---

70 Directive 95/46/EC, Article 2(h).
72 Williams (2009b).
73 See IP/09/570.
74 IP/09/1626.
Three wise monkeys of net neutrality

consent to intercept has freely been given under RIPA. RIPA obviously pre-dates the EPD. This is contrary to the EPD, which defines consent as being ‘freely given, specific and informed indication of a person’s wishes’ (Recital 17);

• UK laws prohibiting and providing sanctions in the case of unlawful interception were limited to intentional interception only, whereas EU law was wider, requiring Member States to impose penalties for any unlawful interception irrespective of whether it was committed intentionally or not. UK law did not correctly implement confidentiality of electronic communications, and powers to fine in sanctions for breaches by the UK Information Commissioner’s Office (the UK personal data protection authority) were inadequate under Article 28 DPD. 75

European laws designed to protect citizens’ privacy and liberty also include the Framework Directive, which lays down the tasks of NRAs. These include cooperating with each other and the Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to a high level of protection of personal data and privacy and ensuring that the integrity and security of public communications networks are maintained. 76

The referral of the UK to the European Court of Justice reflected the Commission’s view that the UK was breaching its obligations under the DPD and EPD, implemented in the UK through the Data Protection Act 1998 and Privacy and Electronic Communications (EC Directive) Regulations 2003 respectively, stating ‘the Commission considers that UK law does not comply with EU rules on consent to interception and on enforcement by supervisory authorities’. 77 The case therefore challenged much of the legitimacy of the UK communications privacy regime and its powers to enforce those rules, notably by the ICO and the police forces.

The European Commission closed the infringement case on 26 January 2012 in recognition that UK national legislation was amended to properly implement EU law on the confidentiality of communications such as email or internet browsing. 78 Following the Commission’s 2010 decision to refer the case to the Court of Justice of the European Union (CJEU), 79 the UK amended RIPA, removing references to implied consent if the interceptor had ‘reasonable grounds for believing’ that consent had been granted. It also established a new sanction against unlawful interception in Section 1A and Schedule A1 of RIPA, 80 administered by the ICC, who has published guidance with

75 Ibid.
77 IP/10/121.
78 See IP/12/60.
79 See IP/10/1215.
practical information on how it will exercise these new functions.\textsuperscript{81} The maximum monetary penalty that can be imposed by a monetary penalty notice is £50,000 under the amended legislation. The ICC guidance notes at Paragraph 2.15 state that:

The Commissioner shall consider serving a monetary penalty notice on a person only if, after investigation, he is satisfied that: the person has without lawful authority intercepted a communication; the conduct cannot be explained by an attempt to carry out an interception warrant; and the person has not committed an offence under section 1 of RIPA.

The criminal investigation into the Phorm trials was finally abandoned by the Crown Prosecution Service Complex Casework Centre on 8 April 2011, choreographed to match the precise day on which the legislative reform was announced. It argued there were:

several public interest factors against prosecution:

- BT and Phorm received considerable legal advice concerning the use of this software and were advised its use was unlikely to be contrary to section 1 of RIPA. The Home Office also provided informal advice that stated the same. Following the second trial, BT received further and conflicting legal advice that led to it halting the covert trials. As there was no evidence to suggest either company acted in bad faith, it could be reasonably argued that any offending was the result of an honest mistake or genuine misunderstanding of the law;
- Both companies cooperated with the police investigation;
- The behaviour in question is unlikely to be repeated. After the first two trials, BT conducted a further single, public trial of the technology (in late 2008). Phorm now requests the user's consent;
- The trial was of limited duration and limited application. The data gathered was anonymised and processed without human intervention and later destroyed;
- There has already been an investigation by a regulator, the Information Commissioner’s Office, which concluded there was ‘no evidence to suggest significant detriment to the individuals involved’ and took no action;
- There is no evidence to suggest that anyone affected by the trial suffered any loss or harm as a result;
- Taking into account all of the above, a court would be likely to impose only a nominal penalty.\textsuperscript{82}

Note that factors included assessments by the ICO, which was itself considered by the European Commission to have inadequate powers, including the lack of significant capacity to fine the parties for their illegal behaviour. It is

\textsuperscript{81} Interception of Communications Commissioner (2011).

\textsuperscript{82} Crown Prosecution Service (2011).
also noteworthy that in 2009–10 the ICO reprimanded the two IAPs that after discussions had decided not to trial Phorm’s system, with both TalkTalk and Virgin Media being reprimanded for their interception of subscribers’ communications, in experimental applications of anti-net-neutrality blocking of P2P and streaming services (which will likely become illegal under the GDPR). In relation to TalkTalk, the Information Commissioner stated: ‘In the light of the public reaction to BT’s trial of the proposed Webwise service, I am disappointed to note that this particular trial was not mentioned to my officials during the latest of our liaison meetings.’\textsuperscript{83} It may be that it would in any case be illegal to access the type of details accessed by IAPs and Phorm even with subscribers’ consent. The UK authorities did not prosecute for interception of confidential communications by IAPs, preferring to issue warnings.

**Corporate interception on behalf of government**

Academics and legal experts will continue to pore over the legislative and judicial response to mass surveillance by government in the period from 2013, building on the work before Snowden.\textsuperscript{84} I focused in this chapter on its implications for private surveillance of the type used to infringe net neutrality. Rauhofer and the late Casper Bowden remind us that:

> Although EU data protection laws are designed to restrict the private actors handling that data from processing it in a way and for purposes that are unlawful, those laws have no effect on public bodies, including law enforcement and security agencies in third countries whose access to that data may be authorized by the laws of their own countries.\textsuperscript{85}

Brown explains that:

> Following Edward Snowden’s revelations of large-scale Internet surveillance by the US and UK governments, there has been broad discussion of the relative merits of national legal regimes intended to enable necessary and proportionate Internet surveillance by intelligence and law enforcement agencies … One important but under-discussed part of such regimes is a statutory requirement for telecommunications companies to make their networks ‘wiretap-ready’.\textsuperscript{86}

He provides examples from many countries, including the apparently obscure s.94 of the Telecommunications Act 1984. Critically, he explains that:

\textsuperscript{83} Sir Christopher Graham quoted in Beaumont (2010).
\textsuperscript{84} Birnhack (2012).
\textsuperscript{85} Rauhofer and Bowden (2013).
\textsuperscript{86} Brown (2013b).
It enables much more sweeping surveillance than is possible using judicial or administrative warrants (or Mutual Legal Assistance Treaty requests) targeted at individuals or individual services. And by reducing the marginal cost of surveillance, it encourages greater use of it.

I reproduce the Table 8 from Brown as it affects case studies explored in Chapters 6–7 (accurate as at 2013 prior to the wave of legislation that followed the Snowden revelations). Note that most nations have similar laws, which make it a legal requirement that networks for security purposes permit exactly the type of interception that would be illegal for private purposes under net neutrality and other interception laws.

Brown concludes that the:

European Court of Human Rights has not previously shied away from dealing with intelligence issues, commenting in Leander v Sweden on ‘the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it’. It is not inconceivable that the UK’s sweeping Internet surveillance activities will be found, as the Court did in S. and Marper with the UK’s National DNA Database, to ‘constitute … a disproportionate interference’ with privacy that ‘cannot be regarded as necessary in a democratic society’.  

The frustrated censorious politicians who want the ‘wise monkeys’ to speak are both reviewing platform regulation and the E-Commerce Directive in 2016, though note that their 2010 review produced little change. National laws favour their copyright industries, such as the Digital Economy Act 2010 in the United Kingdom or the HADOPI law in France.

Interception of communications has eventually been prosecuted when carried out by private investigators, such as those employed by Rupert Murdoch’s newspapers in the celebrated ‘phone hacking’ affair which included computer hacking. However, this has little relationship to net neutrality discussions, and Murdoch’s part-owned IAP Sky Broadband has not been implicated in interception of its clients’ communications. Note that individuals can bring complaints about alleged illegal interception by public authorities to the Investigatory Powers Tribunal, which publishes its most notable rulings on its website. However, complaints about private parties including IAPs cannot be brought to the Tribunal, but instead to

87 Brown (2013b) (footnotes omitted).
89 See BBC (2013).
90 See www.ipt-uk.com/judgments.asp?view=archive (Accessed 16 September 2016), noting ‘That procedure runs no risk of disclosure of any information to any extent, or in any manner, that is contrary to or prejudicial to the matters referred to in section 69(6)(b) of RIPA and [SI 2000/2665 Investigatory Powers Tribunal Rules] rule 6(1).’
Three wise monkeys of net neutrality

Table 8 Statutory requirement for IAP companies to make their networks ‘wiretap-ready’

<table>
<thead>
<tr>
<th>State</th>
<th>Law</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>Federal Law No. 9.296</td>
<td>1996</td>
</tr>
<tr>
<td>European Union</td>
<td>Council Resolution to implement similar lawful interception capability measures(^a)</td>
<td>1996</td>
</tr>
<tr>
<td>France</td>
<td>Posts and Telecommunications Code §D.98-1</td>
<td>1996</td>
</tr>
<tr>
<td>Germany</td>
<td>Telecommunications Act §88/§110</td>
<td>1996/2004</td>
</tr>
<tr>
<td>India</td>
<td>Information Technology Act: Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules</td>
<td>2009</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Telecommunications Act §13</td>
<td>1998</td>
</tr>
<tr>
<td>UK</td>
<td>Telecommunications Act §94(^b)</td>
<td>1984</td>
</tr>
<tr>
<td>US</td>
<td>Communications Assistance to Law Enforcement Act(^c)</td>
<td>1994</td>
</tr>
<tr>
<td></td>
<td>FISA Amendments Act §1881(^d)</td>
<td>2008</td>
</tr>
</tbody>
</table>

\(^a\) Council Resolution of 17 January 1995 on the lawful interception of telecommunications.

\(^b\) Words in s.94(1) substituted by Communications Act 2003, (c.21), ss.406, 408, 411, (Sch. 17 para. 70(2)) (with Sch. 18); SI 2003/1900, arts. 1(2), 2, 3(1), Sch. 1, Sch. 2 with Art. 3(2) (as amended by SI 2003/3142 Office of Communications Act 2002 (Commencement No. 3) and Communications Act 2003 (Commencement No. 2) Order 2003, Article 1(3)).


Source: Brown (2013b).

the ICO or the police. This confirms the analysis by Bowden\(^91\) that UK law as implemented fails to protect citizens from interception, whether by government or private company, and heralding the European Parliament 2013 decision to:

hold a full inquiry into US surveillance programmes, including the bugging of EU premises … It urged them to examine whether those programmes are compatible with EU law. This element of the inquiry could open up a number of sensitive Signals Intelligence relationships between Europe and the US — particularly the close operational partnership enjoyed by the US, Germany and the UK.\(^92\)

\(^91\) Bowden (2013b).

\(^92\) Davies (2013).
It should be noted that criminal law enters the net neutrality debate in the field of counterfeiting and copyright. Civil liability includes potential to pay damages for every copyrighted item copied, for attorney fees for copyright holders pursuing the case, and for exemplary damages for such ‘wilful’ abuse of copyright. By contrast, until 2012 it was assumed that criminal liability would be limited as in exercising its power to render criminal certain forms of copyright infringement, [the United States] has acted with exceeding caution. However, the proposed extradition to the United States following the January 2012 arrest of Megaupload executives in New Zealand has caused some surprise and uncertainty in the application of criminal law, as it follows a 2005 restatement of enforcement policy. The ‘wilful’ requirement in criminal law must be proved beyond reasonable doubt. Nevertheless, a more aggressive prosecution of counterfeiting and other ‘piracy’ (sic) websites was signalled in 2011 with the taking down of domain names belonging to suspected overseas ‘rogue sites’. The cooperation of several national police forces in the Megaupload case indicates a more general trend towards aggressive policing of counterfeiting. This overtook the controversies in the latter half of 2011 over US Congress and Senate versions of a more aggressive anti-infringement Bill.

As part of the Digital Single Market initiative launched on 6 May 2015, the EC committed to a ‘comprehensive assessment on the role of platforms’, launched on 24 September 2015. As the official title indicates, the consultation is extremely wide: ‘Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy’. In the discussions to amend the E-Communications Framework, large well-resourced European incumbent IAPs see the opportunity to make common cause with mobile operators (and others), in an alliance to prevent transparency and permit filtering. The regulation of the Internet that is rapidly taking place is being driven – unquestionably – by European politicians for public safety reasons. They are erecting entry barriers with the connivance of the incumbent players, with potentially enormous consequences for free speech, for free competition and for individual expression. This may be the correct policy option for a safer Internet policy (to prevent exposing children to illegal and/or offensive content, and to counter serious criminal activity), though it signals an abrupt change from the Open Internet.

94 See Department of Justice (2012).
95 Goldstone and O’Leary (2005).
Three wise monkeys of net neutrality

It is therefore vital that regulators address the question of the proper approach to net neutrality to prevent harm to the current Internet, as well as begin to address the heavier questions of positive – or tiered – breaches of network neutrality. The rise in the number of people using encrypted email, Facebook, MySpace, Wikipedia, Skype, Instant Messaging and other applications has extended so far into mass participation that it has truly affected society and the economy in all its facets. Small businesses and solo home-based workers depend on this tool as a vital part of their participation in the economy. The promise of virtual worlds and massive online collaboration is to extend this impact even further by 2020.

The EC suggests that:

‘Online platform’ refers to an undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups. Certain platforms also qualify as Intermediary service providers. [Examples are]:

- general internet search engines (e.g. Google, Bing),
- specialised search tools (e.g. Google Shopping, Kelkoo, Twenga, Google Local, TripAdvisor, Yelp),
- location-based business directories or some maps (e.g. Google or Bing Maps),
- news aggregators (e.g. Google News),
- online market places (e.g. Amazon, eBay, Allegro, Booking.com),
- audio-visual and music platforms (e.g. Deezer, Spotify, NetFlix, Canal play, Apple TV),
- video sharing platforms (e.g. YouTube, Dailymotion),
- payment systems (e.g. PayPal, Apple Pay),
- social networks (e.g. Facebook, LinkedIn, Twitter, Tuenti),
- app stores (e.g. Apple App Store, Google Play) or
- collaborative economy platforms (e.g. AirBnB, Uber, Taskrabbit, Bla-bla car).
- Internet access providers fall outside the scope of this definition.100

‘Platform’ is a generic term that is applied to very different business models: examples included are aggregators/services such as NetFlix and Spotify, which provide a service to consumers but do not connect parties to create a market (as Amazon or eBay do). It is unclear at the time of writing whether such a vast consultation will result in a revision to the ECD, national tweaks to laws to protect domestic services from overseas deregulated competitors (as with local taxi or hotel associations in France and Italy) or no response at all.

---

100 European Commission, Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, 24 September 2015, with background information at European Commission, Background for the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, 2015.
Given that the antitrust case taken by the EC against Google remains unresolved in 2016, it is clear that another academic may need to write a new book on platform regulation in 2017 or later. Fortunately, the consultation expressly excludes IAPs, which means speculation in this book can be limited.

**Conclusion: regulatory problems in implementing net neutrality**

I continue to argue for a prosumer law (consumer- and citizen-orientated) intervention to protect privacy in net neutrality\(^{101}\). That depends on passing regulations to prevent unregulated non-transparent controls exerted over traffic via DPI equipment, whether imposed by IAPs for financial advantage or by governments eager to use this new technology to filter, censor and enforce copyright against their citizens. Unravelling the previous non-liability regime in which IAPs could act as ‘wise monkeys’ risks removing the wisdom and efficiency of that approach in permitting the free flow of information for economic and social advantage. These conclusions support a regulatory regime involving reporting requirements and co-regulation with, as far as is possible, market-based solutions. Regulatory monitoring of potential abuses, including strengthening investigatory capacity and transparency for end users, is a solution that maintains maximum flexibility and policy choice, while ensuring that any abuses can be quickly detected and dealt with appropriately. Solutions may be international as well as local, and international coordination of best practice and knowledge will enable national regulators to keep up with the technology ‘arms race’.

We should not entrench a privacy-invasive ‘Lex Monopolium’ at the expense of an Open Internet, and the choice is not that drastic: innovation and investment can be encouraged by co-regulatory transparency principles, backed up by a regulator with sufficient comprehension and research into the issues, and teeth that are sharp enough, to make a real political commitment to intervene to protect privacy where economic or social interests dictate. Net neutrality certainly provides an excellent platform to create this wider and better-informed discussion, and to prevent harm to the current intermediary role of IAPs as wise monkeys. In the following chapter, I examine the extent to which the UK regulator has followed net neutrality principles in practice.

---

\(^{101}\) See Brown and Marsden (2013a).