Section 6

Internet Access Services

Overview

6.1 The fixed and mobile services discussed in the preceding two sections of this report are used predominantly for the delivery of internet access services. In this section we touch on some of the issues relating to how these services link consumers to the online services and content they wish to access and, in particular, on the increasing role of regulators and policy makers in ensuring that these services operate in an equitable and open way.

6.2 These services now constitute the majority of traffic delivered over access networks and consumers have become increasingly reliant on them for both economic and social activity. As a result, consumers are becoming increasingly concerned about the quality of their internet connection, in addition to the performance of the more traditional services such as voice telephony. Policy makers have recognised this and taken steps to ensure that all sources of content continue to be generally available to all end users and that particular services or classes of service are not unduly favoured unless justifiably necessary.

6.3 In this section we report on how Internet Service Providers (ISPs) are supporting the delivery of internet services over their networks, including how they manage the flow of data over their networks and how they interconnect with other ISPs, content delivery networks and the wider internet. We also touch on how the new regulatory regime for internet access services aimed at ensuring "net neutrality" is being delivered.

6.4 The highlights are:

6.4.1 **A major package of new regulatory obligations coupled with complementary enforcement powers for regulators is in the process of implementation**. This will result in greater transparency in how ISPs manage traffic, market their services and contract with customers.

6.4.2 **ISPs have already been improving the information they provide to consumers about the use of traffic management on their networks as part of a voluntary Code of Practice administered by the Broadband Stakeholder Group (BSG)[40]**. Current traffic management practices in widespread use have minimal or no impact on most users on fixed networks but, given the fixed capacity and variable demand in specific parts of mobile networks, may have an appreciable effect on mobile users during peak periods in busy areas.

6.4.3 **The amount of internet data being delivered to consumers by major video content providers continues to increase**. The use of content delivery networks (CDNs[41]) also continues to increase: internet content is increasingly being served from caching servers embedded in the ISPs' access networks and provided by the content providers.

[40] See http://www.broadbanduk.org/policies/the-open-internet/open-internet-code-of-practice-2016/

[41] Akamai, Google, Amazon, Netflix and the BBC.

6.4.4 Larger-scale ISPs are progressively **introducing support for the latest IPv6 internet addressing system**;

6.4.5 The **lack of security of Internet of Things (IoT)** and other low cost internet connected devices is leading to their being targeted by malware and their use to launch distributed denial of service (DDoS) attacks, increasing concerns over security of personal data.

EU Regulation on Net Neutrality

6.5 In April of this year, the EU Telecoms Single Market (TSM) Regulation on net neutrality rules came into force in the UK. The regulation introduces new rights for consumers and places certain obligations on ISPs. These rules were introduced to address concerns that ISPs might manage traffic on their networks in ways that would limit competition and innovation, which in turn could lead to consumer harm.

6.6 The rules impose requirements on ISPs in terms of how they can manage traffic on their networks and place transparency obligations on informing consumers how they do so. The rules also place an obligation on regulators to closely monitor and ensure compliance with the rules.

6.7 The relevant provisions in the EU regulation are:

6.7.1 **Article 3** sets out end-user rights to "access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice" when accessing the internet. It imposes specific obligations on ISPs intended to secure this outcome. The obligations cover traffic management practices and commercial aspects relating to internet access services such as the provision of "zero-rated"[42] content.

6.7.2 **Article 4** imposes a range of specific transparency obligations on ISPs in relation to the speed and quality of their services. It also introduces requirements about the handling of complaints and the circumstances under which consumers have rights of redress when an internet access service is unsatisfactory.

6.7.3 **Article 5** requires regulators to monitor and ensure compliance and to report annually to the European Commission on compliance and on the general quality of internet access services. It also reinforces regulators' powers to impose quality of service obligations on ISPs.

6.7.4 **Article 6** requires member states to introduce an effective penalties regime for non-compliance.

The duties on regulators

6.8 In order to provide clarity and guidance to the regulators on their obligations, BEREC, the Body of European Regulators for Electronic Communications, published guidelines in August of this year to National Regulatory Authorities (NRAs) on the implementation of net neutrality. NRAs have a range of new tasks under the Regulation, which fall into two groups.

[42] An online content service is “zero-rated” on an internet access service when use of that content service does not count against the data cap applying to the internet access service.

6.9 Firstly, monitoring and reporting on compliance with the Regulation and the quality of internet access in the country. NRAs must “closely monitor” the quality of internet access, and ISPs’ compliance with the obligations in the Regulation, specifically:

6.9.1 The transparency obligations for ISPs to provide additional information in contracts about the broadband speeds - the minimum, maximum, normally-available and advertised speeds for fixed services; the estimated maximum and advertised speeds for mobile services; to handle consumer complaints about these issues, and provide remedies/redress when necessary.

6.9.2 To ensure that ISPs do not limit end-users’ ability to: access and distribute information and content; use and provide applications and services; and use terminal equipment of their choice, irrespective of the end-user’s or provider’s location or the location, origin or destination of the information, content, application or service, via their internet access service.

6.10 Secondly, enforcement of ISP compliance with the Regulation:

6.10.1 NRAs must enforce the Regulation, investigating complaints or potential breaches identified in the course of monitoring compliance. They may require ISPs to change their practices and impose sanctions in the event of serious breaches.

6.10.2 NRAs must also report annually to the Commission on these issues, with the first report due in June 2017.

6.11 Ofcom will continue to maintain a close dialogue with industry to ensure that the appropriate balance is struck between restricting ISP practices, in order to protect innovation in online services, and allowing ISPs to evolve their networks and the range of internet and non-internet services they offer – whilst avoiding harming incentives to invest and ensuring the Internet remains an open and innovative environment.

Implementation actions

6.12 Ofcom currently has an on-going programme of work that is in line with the requirements of the EU Regulation. This programme includes reviewing the voluntary Broadband Speeds Code, and establishing a process to discharge our obligations with regard to the measurement and reporting on the quality of Internet Access Services (IAS).

6.13 Article 4 requires ISPs to ensure that any contract which includes IAS specifies the following:

6.13.1 How traffic management measures could impact on the quality of IAS, the privacy of end-users and the protection of their personal data;

6.13.2 Any impact of fair usage policies, data caps and specialised/managed services on IAS;

6.13.3 Important broadband speeds for both fixed and mobile networks; and

6.13.4 The circumstances under which consumers should be able to exercise their rights of redress, and the remedies available to them, when an internet access service (IAS) is unsatisfactory.

6.14 ISPs also need to have transparent and efficient procedures for handling complaints about such matters.

6.15 Ofcom is currently checking the compliance of the UK's main ISPs' residential consumer contracts in relation to the impact of traffic management on the quality of the IAS and on privacy and the protection of personal data.

6.16 We already have an active monitoring and enforcement programme covering providers' obligations under General Condition 14.4 in relation to complaints handling, including for IAS. We will continue to actively monitor communications providers' (CPs) compliance with these obligations, considering formal enforcement action if breaches are identified.

6.17 We will be revising the Broadband Speeds Codes of Practice for businesses and residential consumers. We aim to strengthen the Codes and ensure that speed information given at point of sale and after sale is in line with the specification of the TSM regulation and consistent across CPs. This will ensure more realistic estimated speed measures are given to consumers, as well as an easier route to redress. The Codes will provide guidance to CPs on the interpretation of the TSM regulation in the UK. We are currently engaged in discussions and workshops with CPs and aim to consult on the revised Codes and guidance in summer 2017.

6.18 In this context, it is worth noting that the Advertising Standards Authority (ASA) recently published research into consumers' understanding of broadband speed claims made in adverts[43]. The study was commissioned following growing concerns that consumers were misled by adverts for broadband services citing headline speeds that customers did not actually receive.

6.19 The research found that speed is an important factor for a significant proportion of consumers who are making decisions between providers. However, levels of knowledge and understanding of broadband speeds vary, and are low overall with many not knowing what speed they need to carry out daily online tasks

6.20 Most understand that the higher the number in the advertisement, the higher the speed of the service, but many are unclear on what this means for them and what speed they would likely achieve. Despite that uncertainty, most consumers believe they are likely to receive a speed at or close to the headline speed claim when, for many, that is not likely to be the case

6.21 As a result, the ASA is reviewing its guidance to advertisers on broadband speed claims. A report will be published in spring 2017. Ofcom will work with the ASA to ensure consistency of approach.

Traffic management practices

6.22 Traffic management is a necessary aspect of ISPs' network management practices. Better controlling the flow of traffic across an ISP's network by using traffic management (TM) can benefit consumers by improving the performance of their broadband connections at peak times. However, there are concerns that through their use of it, ISPs might manage traffic on their networks in ways which can cause consumer harm or limit online innovation. These potentially harmful practices may

[43] See https://www.asa.org.uk/News-resources/Media-Centre/2016/ASA-calls-for-a-change-in-the-advertising-of-broadband-speed-claims.aspx#.WDxjtX2uqgE

include ISPs restricting or 'slowing down' subscribers' access to specific online content, in order to further their own commercial interests, or attempting to charge CPs to access their subscribers. Practices such as these can stifle innovation, be considered anti-competitive and could restrict freedom of expression.

6.23 In light of this, Ofcom has required ISPs to be fully transparent in what they do in this regard, to ensure that consumers can make informed decisions. Before the coming into force of the European Union Telecoms Single Market (TSM) Regulation, ISPs in the UK were already subject to a regulatory obligation[44] to be transparent with consumers about their TM practices. There is an industry-wide code of practice explaining how they should comply with this obligation (the Traffic Management Transparency Code of Practice[45]) which requires that each ISP publish a table summarising its TM policy for each package on offer. These tables have been available on signatories' websites since July 2011.

6.24 In late 2013, Ofcom conducted research on consumer awareness and use of the TM information provided by ISPs. It found that, while the information provided by ISPs was largely accurate and understandable, consumer awareness of TM generally was low. Following this, during 2014 we worked with ISPs to help them improve the impact of the information they provide, with a focus on improving consumer awareness and usability.

6.25 This work, pursued via the BSG Open Internet Forum has resulted in voluntary agreement by the ISPs that they adopt a common approach to defining the traffic management techniques they deploy. The ISPs now provide introductory information explaining their policies and the impact of these policies on their services, and have updated their websites to include glossaries of technical terms.

6.26 We review these key facts indicators and report on them each year as part of this report. Our conclusion is that, broadly, transparency about TM practices has improved, and in general TM policies are less restrictive than they were a few years ago.

6.27 For many fixed networks, TM policies are rarely if ever invoked, although CPs do publish what they would do if networks are congested to ensure adequate performance for time critical applications. Virgin Media continues to apply TM to very heavy data users as part of its demand management policy during busy periods

6.28 Mobile networks also now generally claim not to use TM unless congestion becomes an issue, but this can happen both as a result of normal "time of day" variations in overall loading and as a result of more random increases in users and consequent traffic in particular geographic areas and the cell sites that serve them. They also use data caps and speed limits as another means of managing demand, which may have a much more fundamental impact on the customer experience

6.29 Ofcom continues to explore how best to assess and measure the mobile broadband consumer experience. The "Smartphone Cities, Measuring 4G mobile broadband and voice performance" report[46] that is being published concurrently with this report looks

[44] General Condition 9.2e

[45] http://www.broadbanduk.org/wp-content/uploads/2013/08/Voluntary-industry-code-of-practice-on-traffic-management-transparency-on-broadband-services-updated-version-May-2013.pdf

[46] https://www.ofcom.org.uk/research-and-data/broadband-research/smartphone-cities/december-2016

at how each of the MNO networks performs in a number of major urban areas. In addition to average speed measurement and key web service delivery performance, it has established that generally users in all of the cities can expect to receive more than 2Mbit/s for 90% or more of the time. Whilst this seems likely to deliver a good quality of experience for users, it does emphasise that congestion and, hence, TM can have a significant impact during peak periods or other congestion episodes.

6.30 As mobile networks, and the customers who use them, complete the transition to a fully 4G environment, voice services will be delivered using 4G voice or VoLTE technology, as discussed in Section 5. Since voice will now be transported as any other data service session, ensuring prioritisation during busy periods or localised congestion will become more important, particularly for calls to the emergency services. Ofcom will continue to monitor TM application in this context to ensure voice service quality is maintained.

Internet interconnection trends

6.31 As part of our information requests to communications providers, we asked them how they connect their customers to the rest of the internet. In previous years we have used this information to review and report on the nature of the connection arrangements used by ISPs to deliver internet content.

6.32 Interconnection can be defined as a business relationship where there is an exchange of customer traffic, between administratively separate Internet networks. As referred to in last year's report, there are many different ways in which ISPs can exchange their customer's traffic with each other. These include transit, public and private peering and the deployment of CDNs.

Peering

6.33 With peering, both parties tend to meet at a carrier neutral location known as an internet exchange point or IXP. At this exchange they are able to connect either directly or via the exchange’s equipment. The latter is often known as public peering, the former as private peering, this term also being used to describe interconnection at one or other of the parties own premises.

6.34 In the case of public peering each ISP pays its own costs for connecting into the exchange's switch. In the case of private peering there are many commercial alternatives available to them, which in many cases may depend on the ratio of traffic exchanged between the two parties.

6.35 In the situation where the ISPs exchange traffic within a given ratio they cover their own interconnection costs, as the relationship is mutually beneficial and is considered a “balanced” peering.

6.36 With larger content providers, the ratio between the traffic sent by each of the peers is now typically relatively high and very different from the 1:1 ideal of “balanced” peering, as a content provider such as Netflix sends a significantly larger volume to the ISP's customers than *vice versa*.

6.37 Generally, in the scenario where the amount of traffic exchanged between the ISPs falls outside of the agreed ratio, the ISP responsible for sending excess traffic is likely to have to pay for the excess, as the relationship could be considered as being more beneficial for only one party. This change has led to a “settled” peering model, where billing is based on the out-of-ratio traffic.

6.38 However, in time this trend may reverse, with the increase in cloud computing and other consumer oriented and services that involve bigger uploads, the traffic flowing upstream to some content providers may tend more toward a balanced ratio. This is likely to result in further adjustments to commercial arrangements with both parties sharing the costs more evenly.

Transit

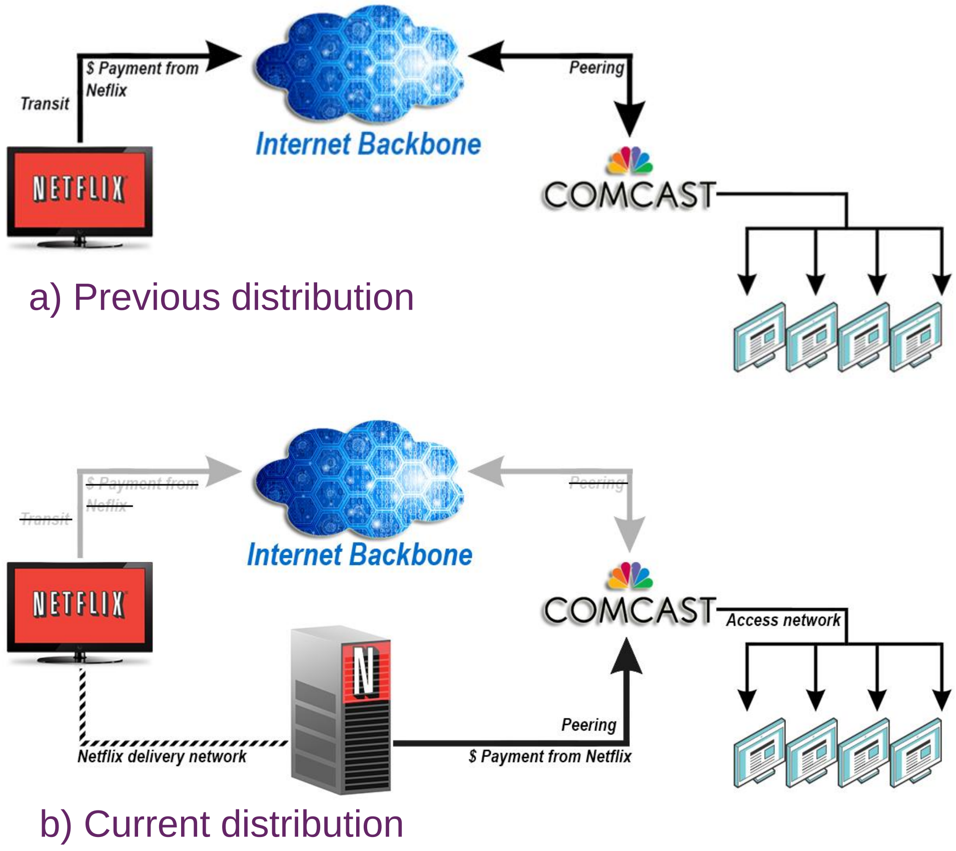
6.39 Transit is when a party pays for access to either all possible destinations in the Internet, or only within a geographic region i.e., destinations with the UK only. The commercial details may include the volume of traffic exchanged or where the customer commits to maintaining a minimum volume.

Content Delivery Networks and caching

6.40 Over the last year, and as we have reported in previous years, both the number of transit and peering connections have been decreasing whilst the deployment of Content Delivery Networks and associated caching has been noticeably increasing.

6.41 Some of the largest content providers now operate their own delivery networks, which must interconnect with ISPs in order to deliver content to consumers. They can do this either by paying a transit network, which itself connects to the ISP, or by interconnecting directly as shown in Figure 28. Direct interconnection is cheaper (for the content provider) for the delivery of large volumes of data

Figure 28: Changing approaches to interconnection



a) Previous distribution

b) Current distribution

Source: Ofcom

6.42 Particularly in the US, these 'direct' interconnection agreements between ISPs and content delivery networks have led to allegations that ISPs are attempting to become *gatekeepers*, extracting a charge from content providers to allow them to access the ISPs' subscribers. The allegations are particularly prominent in those countries (like the US) where there is limited competition among ISPs, and hence the negotiating position of content providers is seen to be weaker.

6.43 In fact, these arrangements are arguably no different from traditional network operator interconnection negotiations and arrangements that have always existed. We have no reason to believe that UK ISPs are abusing their position to extract payment from content providers.

6.44 In particular, we note that Netflix's CDN arrangements, and those of other leading content providers, are now being further extended into the access provider's own network using 'caching servers'. Caching servers are CDN servers which can be placed within the ISP's network or on a third-party network, storing the most popular content. This removes the need for the ISP to connect to the original source of the content every time a customer requests it.

6.45 There are many reasons why this approach may be preferred. The local delivery of content can result in better delivery times to the consumer, which may translate to a better quality of experience, and so is often a preferred option for content providers. This approach further reduces transit or backhaul connectivity costs, and can also improve the customer experience by reducing the likelihood of data congestion in these parts of the network. The commercials in this model are likely to include location services and port-based pricing.

6.46 This evolution is explored further in an academic paper called "Open Connect Everywhere: A Glimpse at the Internet Ecosystem through the Lens of the Netflix CDN[47]" published this year by a team at Queen Mary University of London. This notes, in particular, how Netflix as a content provider has moved to operating its own CDN whilst generally relying on third party cloud storage and, increasingly, caching servers it embeds in ISP networks. The variability of its network interconnection scenarios reflects the very differing network topologies and traffic flows in different markets.

6.47 Many CDN providers are now measuring and reporting on the performance of their content through each ISPs network. The publishing of this data on their websites may also influence how ISPs choose to interconnect with them.

Overall trends

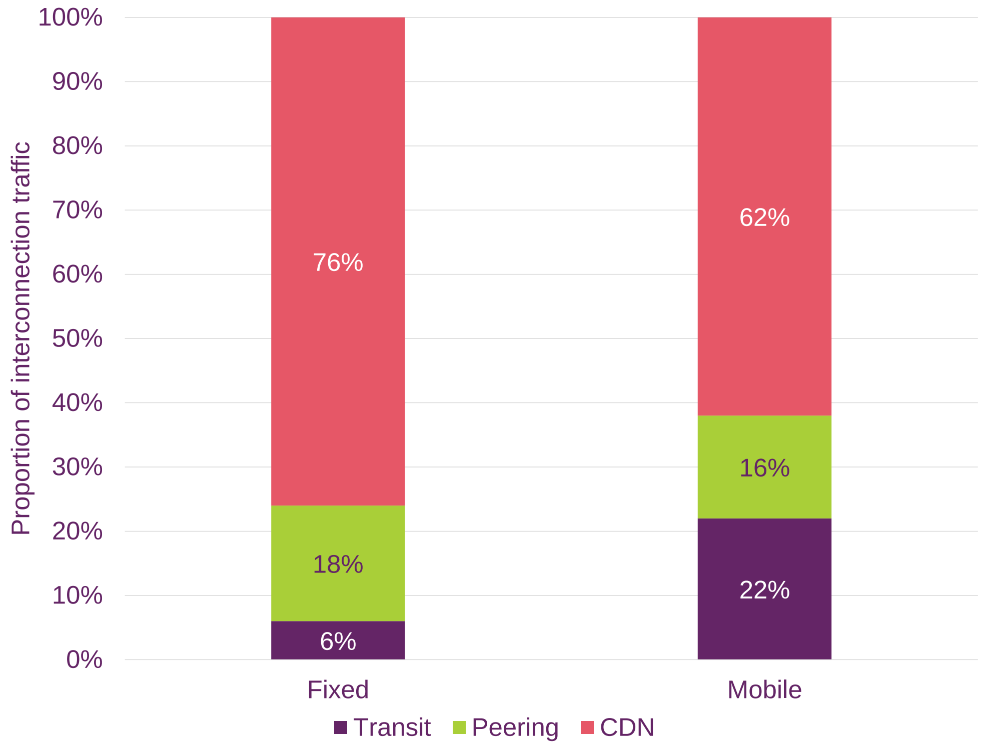
6.48 Last year we noted an increasing use of content delivery networks (CDNs) and direct connections between the access providers and the providers of content and services, and a reducing use of transit and public peering arrangements to deliver internet content.

6.49 This trend has continued - volumes of traffic across the interconnection points between the main ISPs and the internet core, other ISPs and the main providers of content have increased by around 45% since last year.

[47] See http://www.theregister.co.uk/2016/06/22/boffins_map_netflixs_open_connect_cdn/ and http://eecs.qmul.ac.uk/~boettget/mapping-netflix-coseners16.pdf

6.50 As Figure 29 shows, CDN connectivity is an even bigger proportion of the overall traffic than before, although there are notable differences between content providers. Generally, mobile networks have a lower proportion of CDN delivered traffic, probably reflecting the lower consumption of streamed video through devices connected directly to the mobile networks (as opposed to Wi-Fi).

Figure 29: Breakdown of fixed and mobile interconnection traffic



Source: Ofcom analysis of operators' data

Further progress on migrating to IPv6

6.51 The availability of IPv6 to consumers is progressing. IPv4 address ranges are nearing exhaustion and new service deployment is inevitably going to increase the demand for unique, publicly accessible addresses that only the IPv6 regime can deliver. This will, in particular, facilitate the deployment of the Internet of Things (IoT).

6.52 According to the Akamai IPv6 Adoption[48] table, the UK is currently in 10th place in a list of countries who have adopted IPv6. However, compared to last year, most of the major ISPs have now launched IPv6 services to those customers who want it, building on the IPv6 support they already had in their core networks.

6.53 For example, Sky has progressively enabled "dual-stack[49]" IPv6 for approximately 90% of its customers by upgrading the firmware in existing routers. A small percentage of the remainder will need replacement routers as the existing units will

[48] https://www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp

[49] Dual-stack means that those with IPv6 addresses will be able to access both IPv4 and IPv6 sites. This is important as much of the Internet is still on IPv4 only.

not support IPv6. BT is adopting a similar path with their integrated Home Hub routers being mainly IPv6 compatible with a firmware upgrade that is shortly being rolled out.

The Internet of Things - is security an afterthought?

6.54 Recently there have been a number of security breaches where Internet of Things (IoT) devices have been hijacked and used to create distributed denial of service (DDOS) attacks. One particular attack rendered Akamai helpless when they were unable to mitigate the effects of the attack on a target they were providing hosting and network security services for, and the website had to be shut down[50]. In the wake of these attacks, the security, or lack thereof, associated with IoT devices is gaining public interest.

6.55 As the adoption of IoT technologies continues to increase, the threat of security breaches is likely to rise, particularly as some IoT device manufacturers are not currently implementing particularly effective security measures into their products and, in many cases, do not have entirely convincing approaches to firmware upgrades and patching in the light of emerging threats.

6.56 In some cases, the most fundamental problems with these devices can be partly attributed to the default passwords not being changed, thereby allowing hackers to remotely gain access and install malware on them. These infected devices are then used directly or indirectly to launch DDoS attacks.

6.57 The lack of security with these devices may also have an impact on the consumer's privacy, with hackers being able to gain access to personal information. Depending on the IoT device they have, it may reveal personal data related to their health, or their habits of when they leave and arrive home, leaving them vulnerable to higher insurance costs or targeted burglary.

6.58 Many creators of IoT devices, who are not security minded, may be unaware of how vulnerable their products are to cyber-attacks. The GSMA[51] has produced security guidelines on how developers of IoT devices can incorporate security safe guards into their products.

6.59 As the deployment of IoT continues, Ofcom will work to ensure that industry addresses the need to protect the consumer from data exfiltration and other exploits. This could involve educating consumers on how best to protect their devices and personal information.

6.60 The past year has seen a 34% increase in the number of IoT devices individually connected to mobile networks (with a dedicated SIM card) in the UK, as shown in Figure 30 below. The amount of IoT traffic carried over the mobile networks is steadily increasing. However, as the volume of traffic generated by IoT devices is very small, this remains only a small proportion of traffic overall. Figure 30 does not include those IoT devices that are not connected to mobile networks, such as those connected via short range links (e.g. Bluetooth) or wide area low power networks (such as Sigfox).

[50] http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html
[51] http://www.gsma.com/connectedliving/future-iot-networks/

Figure 30: Number of connections and proportion of total data traffic for IoT devices connected to mobile networks

	2016	2015
M2M (IoT) connections	6,999,287	5,212,304
Change	34.3%	28.2%
Average proportion of M2M data to total traffic	0.23%	0.16%
Change	44%	78%

Source: Ofcom analysis of operator data