



# The Consumer Perspective

Response to the Department for Culture, Media and Sport's Discussion Paper for the Communications Review

September 2012



# Contents

Section		Page
1	Introduction	1
2	Prospective market developments and the need for consumer empowerment, protection, and citizen access and inclusion	2
3	Responses to DCMS questions	7
<b>Annex</b>		<b>Page</b>
1	Lost and stolen mobile phones	22
2	Smartphone security	23

## Section 1

# Introduction

- 1.1 Ofcom welcomes the publication by the Department for Culture, Media and Sport (DCMS) of the discussion paper to accompany its Communications Review seminar on the consumer perspective on 4 July 2012.<sup>1</sup> We were also happy to participate in that seminar.
- 1.2 In this response to the discussion paper, we set out the issues which we think are most important for consideration from the consumer perspective in the legislative process. We do this with reference to possible market development and risks of consumer harm which we have identified. For the most part, we think that the current legislative framework works well for consumers, and we believe that the principles underpinning this and much of the provision for consumer empowerment and protection can be carried forward into any future regulatory regime.
- 1.3 We then respond to each of the questions DCMS has posed in the discussion paper. In doing so we build on the material we presented at the seminar, and include additional material which was not covered in the discussion there. Where detailed information is provided in response to questions, we have included this in annexes.

---

<sup>1</sup> [http://dcmscommsreview.readandcomment.com/wp-content/uploads/2012/06/seminar1\\_consumers\\_paper\\_alt.pdf](http://dcmscommsreview.readandcomment.com/wp-content/uploads/2012/06/seminar1_consumers_paper_alt.pdf).

## Section 2

# Prospective market developments and the need for consumer empowerment, protection, and citizen access and inclusion

- 2.1 Our starting point for consideration of the consumer perspective in the Communications Review is that the current framework under the Communications Act 2003 is working well.<sup>2</sup> Our principal duty under section 3(1) of the Act is focussed on the interests of Citizens and Consumers, meaning that those interests are at the centre of our mission. This has provided a consumer focus for our work across the sectors and markets we regulate which we believe is also appropriate and necessary for the future. We therefore think it is important that any new legislation should be framed around the citizen and consumer interest.
- 2.2 Certain requirements will remain constant. For example:
- 2.2.1 Markets will work better if consumers are empowered to engage effectively. This means they must have access to accurate information in order to make decisions in the market, and must be able to act on those decisions (e.g. by switching providers). They must have access to effective mechanisms for redress when things go wrong.
  - 2.2.2 Consumers must be protected effectively against unfair practices.
  - 2.2.3 Citizens should not be excluded from the benefits of communications markets.
- 2.3 However, these requirements will need to apply in new contexts as markets, services and consumer behaviour change in the future.

## Market developments

- 2.4 In considering how consumers will need to be empowered and protected in the future, it is necessary to think about how markets and services may develop, how consumers might respond, and whether there are risks that new forms of consumer harm may emerge from these developments.
- 2.5 It is a fairly obvious statement that the future is hard to predict. In fact, the one thing about which we can be reasonably certain is that technology and services will move in directions which we cannot predict during the period the next Communications Act will be in force. This means that the regulatory framework should be flexible to ensure that consumers can engage effectively with the market, and are adequately protected in scenarios which we cannot anticipate. The current framework works reasonably well in this regard through the general authorisation system, and our ability to make and enforce General Conditions in response to evidence of consumer

---

<sup>2</sup> <http://www.legislation.gov.uk/ukpga/2003/21/contents>

harm, which is part of the overarching European Union (EU) regulatory framework for electronic communications.

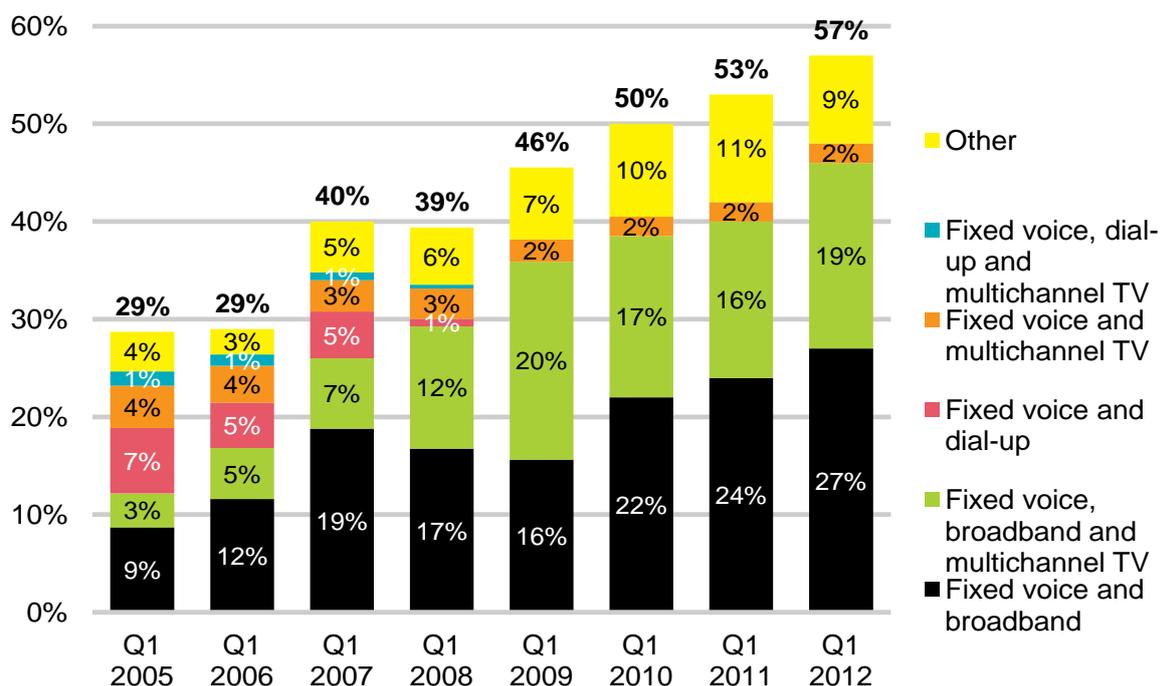
## **Consumer Empowerment**

- 2.6 Two major drivers of consumer empowerment in the market currently are the ability for consumers to clearly understand the options available to them in a competitive market, and to switch between providers (i.e. to make and act on effective choices). For this reason, our current approach to consumer empowerment centres on consumer information and switching. We expect this to continue to be important.

### Switching

- 2.7 We think switching will continue to be important and may even grow in importance as service providers are increasingly able to segment their customer base in ways which enable them to distinguish between high value active customers with a higher propensity to switch, and less engaged consumers. This is likely to result in an increasing focus by service providers on retention of those customers through discriminatory pricing or other enticements. In this scenario, it is likely that active consumers will benefit from targeted efforts to retain their custom, but there are also risks associated with this as follows:
- 2.7.1 First, there will be a natural incentive for large providers to make switching difficult or inconvenient as part of their strategy to retain their most valuable customers. This is a risk that this will reduce competitive intensity in the market.
  - 2.7.2 Second, segmentation may result in an inability for less active and engaged consumers to access good value offers, or in extreme cases even services.
- 2.8 We think the first of these risks can be mitigated by ensuring that switching processes are efficient and do not result in service losses or 'hassle' which will discourage switching, and that consumers are protected from unfair contractual lock-ins.
- 2.9 For these protections to be effective in the future, it is important that the regulatory framework for consumer protection applies consistently across services and sectors in communications markets. This is particularly important as consumers increasingly purchase bundles of communications services. As shown in figure 1 below, currently the most popular service bundles comprise fixed line voice and broadband services, with growth of 'triple play' bundles of fixed voice, broadband and pay-TV.

**Figure 1: Take-up of bundled services over time**



Source: Ofcom technology tracker. QG1. Do you receive more than one of these services as part of an overall deal or package from the same supplier?. Base: All adults aged 16+ (n = 3772)

- 2.10 The availability of bundles has provided convenience for consumers, but also makes switching difficult because different switching processes apply to each component of the bundle. Where regulatory intervention is needed to ensure switching works well, there is a case for this to apply consistently across all services to ensure that the switching experience is not constrained by a single component even where a regulatory remedy has been applied to improve switching across the other services in the bundle.
- 2.11 We must also be mindful that switching barriers will take new forms in the future as customer retention strategies move from a focus on networks and services to a focus on applications which can be tailored to the individual. One area in which there is a danger that barriers to switching will emerge is in the growing ability of service providers to hold service specific data for individual consumers or to control the format of such data. Examples are personal profile data on social networking sites, or media files held either on a personal device or in ‘the cloud’. This data can be difficult to move between providers, particularly when providers are vertically integrated to different formats. The creation of a regulatory framework with adequate safeguards against data lock-in is an important challenge.

### Customer segmentation could lead to exclusion

- 2.12 As noted above, personalisation of services and more sophisticated customer segmentation capability is leading communications providers (CPs) to focus increasingly on selected groups of customers. Commercial customer retention efforts may result in benefits to these customers (e.g. discounts and loyalty rewards), but

there is a risk that other groups of consumers are increasingly 'ignored' by the market. This could give rise to a regulatory need to protect vulnerable consumers.

- 2.13 We believe it is important that the new legislative framework includes appropriate provisions to ensure that all citizens can benefit from communications technology and services. Much of the current framework is centred on fixed voice as an essential service. New legislation should recognise the benefits both to individuals and to society of broadband connectivity and services and of mobility. The debate on 'essential services' will need to take account of the EU regulatory framework and its definitions, but the Communications Review should, in our view, aim to ensure that regulatory asymmetries do not exist in future between different services which are equally useful or essential to individuals and to society.

## Consumer Protection

### Protecting users of legacy regulated services

- 2.14 As the trend away from current interfaces continues, some core regulated services (e.g. voice on the public switched telephone network) will increasingly be regarded as legacy. Consumer protection challenges are likely to emerge from this. For example:
- 2.14.1 As new networks and platforms grow so legacy networks will be de-commissioned raising issues about the migration of consumers from legacy networks.
- 2.14.2 Where legacy networks persist, falling volumes will drive up unit costs and hence put upward pressure on prices.<sup>3</sup> Current protections for vulnerable users would not be well targeted to protect all remaining users of these services. It is therefore possible that we will be called upon to develop new forms of protection at the retail level in addition to universal service requirements – for example, to ensure that services remain affordable for vulnerable consumers. This issue is already live for postal services and is likely to become so for legacy electronic communications services.

### Services and customer relationships will move away from authorised providers

- 2.15 In considering how to ensure consumers are empowered and protected in the future we need to look at how services may be provided and by whom. Suppliers at various points in the value chain have sought to gain ownership of the primary customer relationship in a number of ways, e.g. through vertical integration, development of powerfully branded content or applications, service bundling or combinations of these things. These dynamics have delivered benefits to consumers through the increased functionality and price discounting associated with bundling, and the diversity of capability and consumer experience available through the ever increasing number of services and applications. We expect this commercial push to continue, with the trend towards branded applications as a strong driver of customer relationships and loyalty. In an all IP environment, communications functionality will increasingly be driven through applications and services provided 'over the top' (OTT), but at the same time traditional interfaces may remain important for some consumers. For example, voice communications will be provided in combination with other applications or services (like the current Facebook/Skype combination), but some

---

<sup>3</sup> We can already see this, for example in the network charge controls [http://stakeholders.ofcom.org.uk/consultations/review\\_bt\\_ncc/statement/](http://stakeholders.ofcom.org.uk/consultations/review_bt_ncc/statement/), and in payphone usage. There is also a strong read across from postal regulation.

consumers may prefer to use a traditional telephone handset in combination with a voice only channel (or emulation of a voice only channel).

- 2.16 The trend to applications based services will also continue to shift the focus of communications services from households to individuals. This trend has been evident since the advent of mobile telephony in the 1980s, and is now accelerating as portable personal devices become an increasingly prevalent mode of communications, online activity, gaming and even watching movies. Personalisation of services and more sophisticated customer segmentation techniques are leading CPs to focus increasingly on selected groups of customers.
- 2.17 The consumer experience of “apps for everything” already blurs the boundaries between markets and even sectors. This is particularly so with smart devices which provide seamless access to apps and services provided from multiple sources/networks. The identical touch of a button interface on such devices is likely to increase the level of functional equivalence between traditional voice service and OTT IP voice services. This easy access is quick and convenient for consumers, but it presents challenges for regulators and policy makers using traditional methods to identify markets and regulate them where there is a need to do so.
- 2.18 One of these challenges results from the increasing ‘distance’ between services and networks which means that communications services are increasingly provided by firms which do not (and do not need to) hold any licence or authorisation in the UK and hence are unregulated by us. Often these services are provided OTT.
- 2.19 There is a danger that consumers will be denied access to these services by discriminatory blocking of apps/service by distribution channels. This is a risk we are already managing through our work on traffic management.
- 2.20 A more difficult issue is whether regulation will be able to empower and protect consumers as services are increasingly provided from sources which are currently unregulated. In considering this, we must acknowledge the real risk of regulatory failure – and even perceived regulatory risk – negatively affecting incentives to innovate. This must be balanced with the need to protect consumers where currently regulated services move into the ‘unregulated zone’ as they increasingly are and will continue to as consumers trend to accessing communications services via apps or OTT delivery rather than from regulated providers.
- 2.21 We believe that the Communications Review should consider whether and how to establish an appropriate method of regulation for these services. There may be adequate solutions which stop short of direct regulation (e.g. of intermediary points in the value chain) – for example the provision of information to enable consumers to identify clearly what is in and outside regulatory scope, and hence where safeguards apply.

### Targeted improvements to consumer protection

- 2.22 There are some areas of consumer protection where our experience tells us that improvements to the current legislative framework are needed, and the Communications Review is a great opportunity for this. For example, our work on unexpectedly high bills has highlighted that consumers face unlimited liability for calls made on lost or stolen devices. This puts them in a disadvantageous position relative to lost credit cards for which liability is capped at £50. This issue is explained in more detail in Annex 1.

## Section 3

# Responses to DCMS questions

## Protecting and enabling consumers

Question:

What evidence is there to support concerns from some quarters that the needs of businesses, as consumers of communications services, are not duly being taken into consideration by the regulator?

### Our response

- 3.1 Section 3(1) of the Communications Act sets out our principal duty as being to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition. Therefore outcomes for citizens and consumers are always central to our decision making. Although the interests of citizens and consumers are not always aligned, we consider this dual duty to be appropriate and effective in providing a framework for delivering positive outcomes to the users of communications services and wider benefits to society as a whole.
- 3.2 This dual duty is supported by other relevant statutory provisions, including section 3(4) of the Act which requires us, in performing our duties, to have regard to the opinions of consumers (see definition below) in relevant markets and of members of the public generally. Likewise, section 3(5) requires us, in performing our principal duty, to have regard, in particular, to the interests of those consumers in respect of choice, price, quality of service (QoS) and value for money.
- 3.3 More specifically with regard to business consumers, section 405(5) of the Act sets out that the definition of “consumer” includes business consumers, as well as individuals in their personal capacity. So our duties in respect of consumers as defined mean that, in exercising our functions, we take into consideration the needs of businesses as consumers of communications services.
- 3.4 In particular, in connection with our principal duty described above, one of our central roles is to ensure that communications markets work effectively and are competitive. This is one of the principal ways in which we act to address the needs of business consumers. Relevant provisions in the Act in this connection include, for example:
  - 3.4.1 Section 3(4), which also requires us, in performing our duties, to have regard to the desirability of promoting competition and encouraging investment and innovation in relevant markets.
  - 3.4.2 Section 4(3), which requires us to promote competition in relation to the provision of electronic communications networks and services.
- 3.5 As part of this role of regulating communications markets, we must also have regard to the interests of “customers” (as well as consumers). In accordance with the definition under section 405(1) of the Act, these customers include businesses that act as customers of communications providers. This is in line with, amongst other things, the requirement under section 4(7) that we encourage, to such an extent as we consider appropriate, the provision of network access and service interoperability

for the purpose of securing efficiency and sustainable competition, efficient investment and innovation and the maximum benefit for the persons who are customers of CPs.

- 3.6 In these contexts, we have the power to set general conditions on CPs under section 51 of the Act, including conditions making such provision as we consider appropriate for protecting the interests of the end-users of public electronic communications services (which can include businesses in at least some cases), the power to set access-related conditions under section 73(2) for the purpose of securing end-to-end connectivity for end-users, and the power to set SMP (significant market power) conditions under sections 87-93. Our work in these areas therefore assists in ensuring that markets remain efficient and competitive to the benefit of consumers and customers, including business consumers and customers.
- 3.7 Accordingly, the needs of business consumers are a theme that runs through much of our work. Sometimes these needs can differ from those of residential consumers, and where this is the case we are prepared to take a different regulatory approach.
- 3.8 To illustrate these points, much of our competition work brings direct benefits to business consumers. Our programme of market reviews under the EU regulatory framework and the imposition of regulation to promote competition factor in the broader needs of business consumers and help ensure that business consumers continue to have an extensive choice of communications providers that are able to compete to offer effective services to them.
- 3.9 The Business Connectivity Market Review is a good example of the work we undertake to address the needs of business consumers and customers. This is a priority project for 2012/13 that will consider whether regulation is required to address SMP in markets covering a broad range of services used by businesses. This is just one of a number of projects being taken forward this year in which we will look to ensure that outcomes support the needs of businesses of all sizes across the UK.
- 3.10 Other projects include:
- 3.10.1 promoting competition and investment in the delivery of superfast broadband;
  - 3.10.2 auctioning the 800 MHz and 2.6 GHz spectrum bands;
  - 3.10.3 securing the provision of the universal postal service and determining the needs of postal users;
  - 3.10.4 working in collaboration with government and industry to promote widespread superfast broadband and reduce mobile not-spots.
- 3.11 It is also worth noting that much of the work that we undertake under the consumer umbrella more generally is of direct benefit to business consumers, particularly small and micro-businesses. For example, our decision to ban Automatically Renewable Contracts – contracts which tied customers into long-term contracts and limited their ability to switch providers – included a prohibition on such contracts for small business as well as residential consumers.

## Research

- 3.12 We are required, under sections 14 and 15 of the Act, to make arrangements to ascertain the experiences of consumers (including business consumers) in

communications markets, including in relation to complaints handling and dispute resolution, and to take such research into account in carrying out our functions. In accordance with these duties, we take into account the interests of business consumers through our research programme, which is designed to aid our understanding of business needs and the experiences of business consumers.

- 3.13 An example is the Business Consumer Experience, a comprehensive survey of businesses using telecoms services. This provides vital intelligence and has directly informed our decision making in order to ensure that business consumers are able to obtain better outcomes in terms of choice, quality and value for money. Where appropriate, business views are also captured in sector specific research projects such as the Narrowband Market Review and on Post where we are investigating use and satisfaction of postal services amongst UK businesses through our tracking survey. Again, we expect this work will directly inform our decision making.

### Governance and consultation

- 3.14 We are required, under section 16 of the Act, to have in place effective arrangements for consulting consumers (again, including business consumers) in carrying out our functions. In accordance with this duty, our governance structures and the various committees and advisory bodies that assess our proposals and decisions also play a role in making sure that the needs of business consumers are adequately considered. The committees include members with commercial and small business backgrounds who can provide an appropriate level of challenge if the business angle has not been given due consideration. These include the Communications Consumer Panel, the Advisory Committees for England, Northern Ireland, Scotland and Wales and the Ofcom Spectrum Advisory Board. Among these the Communications Consumer Panel has an explicit focus on small business consumers, as required by section 16(3) of the Act.

### Potential modifications in future legislation

- 3.15 While our work does incorporate the needs of business users, we are always open to ways in which we can improve our general approach. However for the reasons set out above we do not think a general amendment giving us new duties with regard to business is necessary. In light of this we would be keen to understand why some stakeholders have formed a view that we do not fully take into consideration the needs of business consumers and to address any gaps.
- 3.16 It is also worth bearing in mind that with regard to our ability to act on behalf of business, in certain cases there are limits to what we can do. For example general consumer protection legislation, such as the Unfair Terms in Consumer Contracts Regulations 1999,<sup>4</sup> is often based on EU law which normally limits the definition of consumer to natural persons not acting in the course of business (the same definition as used in the EU regulatory framework for electronic communications). Similarly, certain other general consumer protection legislation intended to protect businesses, for example the Business Protection from Misleading Marketing Regulations 2008,<sup>5</sup> is enforced by the Office of Fair Trading (OFT) rather than by us.
- 3.17 One area where we think the current legislative framework may merit review is in ensuring there is an appropriate balance around the provisions for large and small businesses. Our duty to make General Conditions relating to customer interests (e.g.

<sup>4</sup> <http://www.legislation.gov.uk/uksi/1999/2083/contents/made>

<sup>5</sup> <http://www.legislation.gov.uk/uksi/2008/1276/contents/made>

on consumer protection issues such as complaints handling and dispute resolution by communications providers) under section 52 of the Communications Act is limited to domestic consumers and small businesses with no more than 10 employees. It may be appropriate to maintain this type of distinction in new legislation to reflect the very different nature of the relationship between suppliers and small and large business customers. For example, large businesses generally have better capability for contract due diligence and are able to negotiate bespoke deals with suppliers, whereas small businesses have more in common with the purchasing behaviour of domestic consumers. However, the 10 employee threshold is somewhat arbitrary and we believe the Government should review this with a view to targeting protections for small businesses more accurately to those which need it.

## The Open Internet

Question:

Are Ofcom's powers sufficient – and sufficiently clear – to address potential future concerns about blocking and other forms of discrimination?

### Ofcom response

#### The policy principles

3.18 The background notes produced for the consumer-perspective seminar identified the increasingly important economic benefits of an “Open Internet” but rightly also noted the emerging tensions between maintaining complete “freedom to innovate” and managing the costs of access delivery within an economically viable envelope. From this starting point a number of key issues can be identified, as laid out in the Ofcom Statement on Net Neutrality published in November, 2011:

- 3.18.1 The benefits of “innovation without permission” are important – consumers value the new services that have arisen as a result of it, and the conventional model of competitive intensity leading to the maximisation of such benefits could break down if access operators were able to discriminate against OTT services unfairly.
- 3.18.2 On the other hand, traffic management can be an entirely legitimate means of optimising network performance, for example by ensuring that the overall bandwidth in an access network and between it and the “rest of internet” is shared equitably between users, with more time sensitive application classes being given some prioritisation if congestion occurs. This may extend to the provision of “managed services” that provide QoS guarantees for high bandwidth applications such as long form broadcast quality video.
- 3.18.3 The best means of ensuring that such traffic management is not unduly discriminatory and in the best interests of consumers is by requiring or encouraging maximum effective transparency of what measures access providers actually apply. This allows consumers to make informed choices between providers, based on what service attributes are important to them, and may provide an evidence base for regulators to determine if the practices adopted are detrimental to the interests of consumers.

### The current position

- 3.19 We have adopted a policy of not pre-judging whether existing traffic management practices are problematic as there is little or no evidence that any significant blocking or extreme “throttling” is currently undertaken, other than the blocking of VoIP (voice over IP) applications by some mobile networks. Our view is that the most appropriate initial regulatory action is to improve transparency, rather than intervene immediately. However, we have stated that we will use the Infrastructure Report Update (IRU) that we are planning to publish in the Autumn as an opportunity to assess and benchmark the current practices used by mass market access providers and provide an initial perspective on whether there are any causes for concern emerging.
- 3.20 The DCMS notes highlight the voluntary Code of Practice (CoP) on traffic management transparency facilitated by the Broadband Stakeholder Group and adopted by all of the key mass market providers,<sup>6</sup> and the Key Facts Indicators whose publication it requires will provide a significant input into our benchmark exercise in the IRU. They also note the more recent work on a CoP on Traffic Management Principles that is aimed at ensuring that the most problematic forms of service blocking or restriction are not adopted.<sup>7</sup> This has proven to be more contentious, with a number of CPs, both fixed and mobile, being unwilling to sign up, and a number of content and service providers maintaining that it does not go far enough in making commitments to eschewing restrictive traffic management practices. (They have particular concerns that use of “managed services” to support access providers’ own-brand content services may disadvantage their OTT offerings.) Nevertheless, DCMS officials and Ministers welcomed it when it was launched on 24 July, and we would concur with that support.
- 3.21 This new CoP emphasises the role that we could play both in analysing market practices with a view to intervention if harm is being caused to consumers, and in investigating specific complaints and disputes between service and access providers, in both cases using our QoS powers under the EU regulatory framework. It also notes that signatories are keen to work with us in developing an effective CoP compliance monitoring and enforcement regime.
- 3.22 We note these observations and can confirm that we are keen to work with industry to ensure both CoPs operate effectively.

### The need for regulatory clarity

- 3.23 Our response to the discussion document’s question is “possibly not”. In our view, the current regulatory powers we have in this area are, at the very least, insufficiently clear to give certainty that we can use them effectively in all likely scenarios.. This lack of clarity undermines the fundamental principle that lies at the heart of EU policy on the Open Internet. Article 8(4)(g) of the Framework Directive,<sup>8</sup> as amended,<sup>9</sup> now includes an objective for regulators to promote the interests of citizens of the EU by:

"promoting the ability of end-users to access and distribute information or run applications and services of their choice"

<sup>6</sup> [http://www.broadbanduk.org/component/option,com\\_docman/task,doc\\_view/gid,1335/Itemid,63/](http://www.broadbanduk.org/component/option,com_docman/task,doc_view/gid,1335/Itemid,63/)

<sup>7</sup> [http://www.broadbanduk.org/component/option,com\\_docman/task,doc\\_view/gid,1340/Itemid,63/](http://www.broadbanduk.org/component/option,com_docman/task,doc_view/gid,1340/Itemid,63/)

<sup>8</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:EN:PDF>

<sup>9</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF>

- 3.24 The EU regulatory framework does provide some associated powers aimed at ensuring regulators can help achieve that objective. In particular, Article 20 of the Universal Service Directive,<sup>10</sup> as amended,<sup>11</sup> plays an important role, by strengthening the minimum contractual protections for consumers across the EU in order to improve the quality of information provided to them. In the UK, we have already modified General Condition 9 to reflect those protections under UK law.<sup>12</sup> That Condition now includes a requirement that new consumer contracts must specify in a clear, comprehensive and easily accessible form:

“information on any procedures put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures could impact on service quality”

- 3.25 Article 21 of the Universal Service Directive, as amended, sets out further minimum requirements related to consumer transparency and publication of information. These enable regulators to set new obligations on communications providers. Article 21 also notes that regulators may, if deemed appropriate, promote self or co-regulatory measures prior to imposing any obligations.

- 3.26 As noted above, we have acted to ensure these new obligations are implemented effectively and believe that good progress has been made around a number of the associated self regulatory initiatives on transparency and traffic management practices. We will, however, continue to assess whether these initiatives are effective and, where appropriate, seek to integrate them into our broader programme of transparency based consumer protection. In particular, the self-regulatory Traffic Management Transparency Code has been in place for over a year, and is due to be reviewed. As part of the research conducted into compliance with our well established Voluntary Code of Practice on Broadband Speeds,<sup>13</sup> we looked at the provision of traffic management information. Compliance with the Traffic Management Code appears to be satisfactory but it remains unclear whether the information provided is easily understood and usable by consumers. This is something we will address with industry over the coming months.

- 3.27 Turning to the regulatory powers of intervention, Article 22(3) of the Universal Service Directive, as amended, sets out a new provision which enables regulators to impose minimum QoS obligations on providers. This was implemented by a modification to Section 51 of the Communications Act,<sup>14</sup> which allows us to set general conditions:

"in order to prevent the degradation of service and the hindering or slowing down of traffic over networks, impose minimum requirements in relation to the quality of public electronic communications networks"

- 3.28 This power provides, in principle, some capability to intervene if industry self regulation and competitive pressure are insufficient to prevent throttling or outright blocking of services to consumers' detriment. Whilst we have not yet concluded that such intervention is warranted, we are clear that the capability of doing so effectively

---

<sup>10</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:EN:PDF>

<sup>11</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF>

<sup>12</sup> <http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/general-conditions.pdf>

<sup>13</sup> <http://stakeholders.ofcom.org.uk/binaries/telecoms/cop/bb/cop.pdf>

<sup>14</sup> <http://www.legislation.gov.uk/ukxi/2011/1210/contents/made>

is an important regulatory “backstop” to ensure consumers continue to benefit from vibrant service innovation.

- 3.29 Clearly, there are a number of potential scenarios warranting regulatory scrutiny that may arise, with a wide variation in services that could be affected by an equally wide range of CP traffic management practices. We plan to analyse these scenarios in detail to determine how the QoS obligations can be applied but already have some concerns that they may not be applicable in some circumstances. Whilst other aspects of the overall EU regulatory framework will allow us to intervene when the service in question is within our general powers to regulate as an electronic communications service, this does not provide us with either the clarity or the consistency across all service types that we believe is warranted.
- 3.30 We are discussing this question with other regulators, but we would note that this potential limitation was not addressed in the work programme of the Body of European Regulators of Electronic Communications.
- 3.31 We believe that this potential gap, if it is confirmed, clearly justifies legislative intervention, provided that this can be done without it running contrary to the relevant aspects of the EU regulatory framework overall. We are keen to share our analysis with DCMS and to work together to determine how best to address the issue if our concerns are well founded.
- 3.32 One additional issue that might warrant some consideration is clarification of our powers to collect data to underpin the publication of reports on service availability, performance and take-up to help facilitate consumer choice and provide better information to other stakeholders. At the moment, whilst we have broad powers to collect information in order to underpin an own initiative investigation, or one triggered by a complaint or dispute, our statutory rights to collect information for publication are less clear. Whilst the Digital Economy Act 2010 did introduce an obligation to publish a report on telecoms infrastructure, with associated statutory rights to collect relevant information, it has a defined triennial periodicity, unless the situation has been deemed to have worsened materially.<sup>15</sup> The removal of this fixed timetable to allow the production of public reports on a more frequent and flexible basis would seem appropriate, given the rapid pace of current and likely future change (such as Next Generation Access and 4G roll-out) and the benefits of better informed consumer choice not to mention policy making.

## Unsolicited marketing calls and spam e-mails

Questions:

Are the current arrangements adequate and, if not, how could they be improved?

What further measures could be considered – especially as spam e-mails mostly originate from overseas?

### Ofcom response

#### Nuisance calls

- 3.33 We share the Government’s concern about the inconvenience, annoyance and distress which consumers are experiencing as a result of nuisance calls and

<sup>15</sup> <http://www.legislation.gov.uk/ukpga/2010/24/contents>

messages. We are particularly concerned by the number of calls and messages caused by companies seeking to generate leads for compensation claims, such as for Payment Protection Insurance mis-selling. We believe there is a need to review the operation of the existing regulatory system to identify the action that could be taken to reduce consumer harm in both the short- and medium-term.

### *Short-term*

- 3.34 There is a need for effective and co-ordinated enforcement action by us and the Information Commissioner's Office (ICO). We will continue to focus on tackling abandoned and silent calls. In April we imposed a financial penalty of £750,000 on Homeserve.<sup>16</sup> We are conducting two more formal investigations at the moment and take informal action by sending warning letters to companies which cause consumer complaints. We have also written to over 120 companies to remind them what they must do to comply with our rules and pointing to the Homeserve decision as evidence of our willingness to take robust action.
- 3.35 The ICO has lead responsibility for enforcing the rules governing unsolicited marketing calls, recorded message calls and unsolicited texts, and we welcome its recent decision to put more resources into this area of work. We will continue to work with the ICO to improve intelligence-sharing and ensure that our activities are co-ordinated.
- 3.36 As well as taking enforcement action against companies which generate nuisance calls and messages, we should consider the need for action against companies (particularly claims management companies) that generate 'leads' from nuisance calls. We believe that there could be value in cross-Government action to examine how the incentives to generate leads might be reduced.
- 3.37 There is also a need to improve information for consumers and make it easier for them to complain. We have been working with the ICO, the Ministry of Justice (which regulates claims management companies) and the OFT (which regulates debt management companies) to develop a consumer guide that is designed to provide a comprehensive source of information about nuisance calls and messages. In relation to each type of call or message, the guide explains what action consumers should take, including who they should complain to. We have shared the draft guide with stakeholders, including consumer bodies, and will take on board their comments in producing the final version. We are intending to publish the guide on our website in Autumn 2012, with links to the Telephone Preference Service (TPS) website and the websites of other relevant regulators. This should make it easier for consumers to find out who to complain to rather than being referred from one body to another. We will also work with consumer bodies to promote the guide and more generally, to help consumers receive useful and accurate information.
- 3.38 We are also aware of concern that recipients of unwanted calls and messages sometimes cannot identify the calling number (known as calling line identification – CLI) or the company behind the call. We have two initiatives that we hope will improve the situation. First, we are encouraging BT to provide international CLI in the way that other CPs do. At the moment, a BT customer that receives an international call will not see the number on their handset display or be able to find out the number if they dial '1471'. This means that they cannot choose to only accept calls from numbers they recognise and if they receive an unwanted call from overseas, they cannot make a note of the number and report it. Secondly, we have asked the Office

---

<sup>16</sup> <http://media.ofcom.org.uk/2012/04/19/homeserve-fined-750000-for-silent-and-abandoned-calls/>

of the Telcoms Adjudicator to work with industry to develop a formal process for tracing and blocking calls. This should enable more rapid action to prevent unwanted calls, particularly from overseas.

#### *Medium-term*

- 3.39 Subject to seeing whether planned action in the short-term significantly reduces consumer harm, we think there would be value in reviewing the current system of regulating nuisance calls and messages and considering whether an alternative model might produce better outcomes for consumers.
- 3.40 In our view, a review should begin by identifying the functions that should form part of the system of regulation. Starting from first principles in this way is likely to lead to better outcomes for consumers than considering how the current system might be adjusted. Our initial thinking is that the following functions should be built into the system:
- 3.40.1 maintaining the TPS register – registering consumers who do not want to receive marketing calls and supplying the register to companies that carry out telemarketing;
  - 3.40.2 consumer information – advising consumers what to do if they receive nuisance calls and messages and who they should complain to;
  - 3.40.3 complaints-handling – handling and recording complaints from the public;
  - 3.40.4 intelligence-gathering – analysing complaints data and data from other sources, e.g. other regulators, market research, stakeholder views;
  - 3.40.5 enforcement – taking enforcement action to prevent and deter consumer harm, which would require powers to carry out investigations and impose tough sanctions;
  - 3.40.6 stakeholder engagement – developing and maintaining strong links with stakeholders, including consumer groups, the telemarketing industry, CPs and regulators; and
  - 3.40.7 strategic leadership – taking a strategic view of the regulation of call centre practices, taking account of the whole value chain, including lead generation companies.
- 3.41 Mapping these functions onto the current system shows that all of them are shared (except the function of maintaining the TPS register). This suggests that there is scope to improve the consumer experience, particularly in relation to complaint-handling, and to achieve greater efficiency in, for example, handling complaints, gathering and analysing intelligence, and co-ordinating enforcement action. As well as considering how best to carry out the requisite functions, we suggest identifying the principles that should be built into any new system of regulation. In our view, the following four principles would provide a good starting point:
- 3.41.1 There should be a central focus on protecting the interests of consumers.
  - 3.41.2 The system should reflect regulatory best practice.

3.41.3 Reputable companies should be able to carry out telemarketing without being damaged by the activities of rogue companies.

3.41.4 There should be adequate and sustainable funding.

## Making digital payments

Question:

Do you have evidence and further views on how such systems could be made more secure, and what could be done to encourage uptake of the technology?

### Ofcom response

3.42 Contemporary smart phone operating systems are highly complex and we believe it is timely for policy makers to consider the security of these systems and whether additional consumer protection is needed. We include a detailed briefing on this in Annex 2.

Question:

Given the potential for growth presented by such convenient, high speed payments, do you have views on the optimal regulatory framework for mobile phone payments?

### Ofcom response

3.43 Payments via mobile phones incorporate a very wide range of platforms, payments and products, and as digital technologies evolve and consumer take-up of smart phones increases we can expect the market to rapidly grow and also for new business models to emerge.

3.44 The Communications Act set out the framework for the regulation of Premium Rate Services (PRS), The PRS regulatory framework is a hierarchy with three components:

3.44.1 *The Communications Act* defines PRS in a broad manner and provides us with the power to set conditions for the purposes of regulating their provision.

3.44.2 *The PRS Condition* which we make defines which subsets of PRS are subject to regulation (i.e. our statutory backstop enforcement powers)<sup>17</sup> – these are known as Controlled PRS. We can change these to include or exclude services.

3.44.3 *The PhonepayPlus Code of Practice*. We have appointed PhonepayPlus (PP+) as the designated agency to deliver day-to-day regulation of Controlled PRS. We have approved PP+'s Code of Practice which outlines wide-ranging rules to protect consumers and the processes PP+ applies when regulating the industry.<sup>18</sup> Again, this can be changed.

3.45 Since the Communications Act came into effect, the PRS market has changed very significantly. A very wide range of services are now billed through the phone bill, including through Payforit, a micropayment scheme created and supported by all of

---

<sup>17</sup> [http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/narrowband/PRS\\_Condition\\_20\\_Dec\\_10.pdf](http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/narrowband/PRS_Condition_20_Dec_10.pdf)

<sup>18</sup> <http://www.code.phonepayplus.org.uk/pdf/PhonepayPlusCOP2011.pdf>

the UK mobile network operators that enables consumers to use their mobile phone account or prepaid balance to transact when purchasing content and services on the internet. Another indication of how PRS services are evolving is evident from the announcement by Telefonica Digital in July 2012 that it had signed global agreements to offer direct to bill payments with Facebook, Google, Microsoft and Research in Motion (RIM)<sup>19</sup>.

- 3.46 However it is also the case that as the market for digital content and services on mobile phones has grown and evolved, a smaller proportion of micropayments fall under the current definition of PRS, which broadly sets as its boundary services paid via the communications network provider (e.g. via a phone bill). Mobile apps stores in particular (such as those via Apple's iOS or the Android OS) have emerged as a way of purchasing digital applications and content, and a wide range of payment mechanisms are used to purchase content including credit/debit cards, mechanisms such as PayPal and virtual currencies.
- 3.47 Micropayments made from mobile phones are therefore an important and growing part of the digital economy. However, the characteristics of micropayment platforms, payment mechanisms and the products and services themselves all contain risk of consumer harm and a clear and understood regulatory framework is necessary to protect consumers and maintain and increase the consumer confidence which is necessary for the industry to continue to thrive. The following characteristics of micropayments all create the potential for consumer harm:
- 3.47.1 *Platform characteristics*: difficulties in identifying from whom redress should be sought (e.g. platform owner vs content producer), platform lock-in and low barriers to entry and exit make it possible for "bad actors" to operate; platform fragmentation increases the chance that a given piece of digital content will not work on a given platform; digital platforms make it easier for private data to be abused between platform provider and content producer; the anonymity of digital platforms makes it easy for minors and vulnerable persons to be exposed to unsuitable content.
- 3.47.2 *Payment characteristics*: complex pricing models can make it difficult for consumers to know how much they are spending; low friction (e.g. 'one click' purchasing) can lead to the consumer purchasing content unintentionally or without being fully aware of what they are signing up for; low price points can lead to impulsive behaviours and 'bill-shock', while consumers are less likely to pursue redress for low value payments unless it can be very easily obtained; automatic expiration on gift cards, intermediate ('virtual') currencies and credits can lead to financial loss for the consumer; storage of credit and debit card details creates risk of hacking and fraud; intermediary currencies (such as Facebook Credits) do not provide the protection of credit card purchases.
- 3.47.3 *Product characteristics*: the nature of digital content makes it difficult to verify that it is fit for purpose prior to sale; digital product retailers have little incentive to encourage digital product 'returns'; there can be a lack of clarity over ownership of digital product ('licensed', 'rented' or 'owned'); digital content frequently has an addictive quality to it; digital content is often attractive to vulnerable consumers who are more likely to suffer harm; anonymity of digital content platforms allows consumers to buy

<sup>19</sup> [http://pressoffice.telefonica.com/documentos/nprensa/Direct\\_to\\_Bill\\_FINAL.pdf](http://pressoffice.telefonica.com/documentos/nprensa/Direct_to_Bill_FINAL.pdf)

'embarrassing' content (e.g. adult), for which they are less likely to seek redress.

- 3.48 A regulatory framework for micropayments should therefore be able to encompass platform, payment and product characteristics. This is the case for current PRS where the protection offered by the PP+ CoP covers all aspects of the purchase experience, including the payment mechanism (i.e. the telecoms operator's billing platform), the contract with the provider (e.g. clear information about pricing and terms & conditions), the technical quality of the end products, the suitability of content and the protection of consumer information. The challenge is to ensure that this same level of protection is available for new types of PRS and PRS-like services.
- 3.49 We have worked closely with PP+ on these issues and have contributed to PP+'s submission to the Communications Review. We fully endorse the analysis and recommendations in the PP+ submission, and therefore do not replicate the details in our own submission.
- 3.50 As detailed in the PP+ submission, we consider that there are two significant outputs from the Communications Review which will prepare the ground for effective regulation of the diverse and rapidly growing and evolving micropayments market.
- 3.50.1 The Communications Review presents an opportunity to update the current regulatory framework for PRS services to ensure that the same level of consumer protection is provided for new types of PRS services that have recently emerged, while it should also be an objective of new legislation to ensure that the regulatory framework is flexible enough to accommodate new services which may emerge and which may potentially give rise to new sources of consumer harm.
- 3.50.2 However, it is also the case that issues related to micropayments extend beyond PRS and beyond those areas which are addressed by the Communications Review, involving issues such as consumer protection legislation and the broader consumer protection framework including trading standards. We recommend that an output of the Communications Review should be stimulation and co-ordination of discussion with industry, consumer groups, regulators and the Government about how wider regulatory and consumer protection frameworks should be updated for the future of digital micropayments.

## Data protection

Question:

How can the appropriate privacy protections and transparency around data be maintained for consumers, whilst ensuring that growth and innovation are not stifled?

- 3.51 These are complementary objectives: privacy protection and transparency are essential to sustained growth and innovation in the use of consumer data: without them, consumers will increasingly reject all such activity.
- 3.52 The wide adoption and broad range of uses made of the internet has enabled a huge increase in the collection and analysis of information about individuals' preferences, behaviours and attributes such as purchasing intentions, hobbies, gender and location. Billions of data-points are gathered and used by individual online service providers like Facebook, and collected and aggregated across multiple sources

(online as well as offline) by data providers and other information intermediaries. This consumer data can be analysed to develop and deliver innovative and personalised services as well as targeted advertising, creating value for service providers and for consumers themselves. However, the gathering and use of such information also gives rise to material privacy risks for consumers.

- 3.53 The policy environment for data protection and privacy is currently under review at the EU level. The dynamic nature of the market and uncertainty about user expectations and risks makes it hard for policy-makers to strike the right balance between supporting growth in an exciting new area and yet still protecting the legitimate interests of users. In particular, the mechanisms through which consumers are informed about data-gathering and exploitation, and the ways in which their consent to such activity is secured, are likely to require continued regulatory scrutiny.
- 3.54 We support the development of innovative data-based services, which potentially support investment by core stakeholders in content and network infrastructure and underpin some of the most widely used services online; but such services must be provided in ways consistent with consumers' rights to privacy.
- 3.55 It is not clear that data markets are working as they should for consumers: many consumers don't really understand what is going on, and in some cases are unhappy with industry behaviour when they find out about it. However, our analysis suggests that the core challenge to the development of these markets is not in the form or extent of the regulations themselves; consumers' rights have been materially extended by the E-Privacy Directive,<sup>20</sup> as amended,<sup>21</sup> and are likely to be expanded further through the proposed Data Protection Directive.
- 3.56 Furthermore, there are considerable efforts under way to improve industry compliance and consumer understanding; and the pace of development suggests that the consumer risks might be transitional rather than enduring. For example, we do not yet know what the impact will be of the widespread changes in provision of information about online cookies which began in May of this year, following the ICO's timetable for implementation of the amended E-Privacy Directive.
- 3.57 However, further significant action by both industry and the ICO will be essential to ensuring that data market actors deliver the levels of consumer transparency and control intended in the regulations, as well as the expected innovation in the provision of services. Without this, in the worst case, a vicious circle of opaque behaviour by industry and declining trust by consumers could wholly undermine development.
- 3.58 The risks of data breaches are also growing in line with the general expansion of data gathering and use; industry, particularly small and medium-sized enterprises, faces challenges in securing advice on, and in implementing robust approaches to, data security.
- 3.59 We do not have lead regulatory responsibility in this area, although we do have a formal role in relation to network security; we will continue to support the fair development of the relevant markets, for example through our programme of research into online audiences' media literacy. We will also seek to extend our relationship with the ICO in areas of common interest.

<sup>20</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:EN:PDF>

<sup>21</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF>

## Purchasing digital content

Question:

Consumers expect a seamless digital experience – they are already accessing digital content and using it on multiple devices. How could this principle be extended to enable them to pay once and have the content available across platforms and networks, and are there barriers to this happening?

- 3.60 In paragraph 2.11, we explain why data portability is important. Interoperability for a seamless digital experience requires a solution to technical, commercial and legal challenges. It should be noted that some of the barriers to interoperability are justifiable commercially and legally. Not all barriers result in harm to consumers.
- 3.61 The market is to some extent addressing some of these challenges – for example by developing software solutions to make content interoperable between competing platforms and devices.
- 3.62 However, barriers to interoperability could still remain a problem for consumers, in particular where those barriers are unfairly preserved to prevent switching – for example where consumers use a bundle of services from a single supplier to manage their data like Apple devices and iCloud.
- 3.63 The framework for interoperability will need to preserve incentives for innovation and investment as well as ensure that consumers are not locked in in ways which are detrimental to competition. It will also need to ensure that personal information data is properly protected where the transfer of consumer data between operators is necessary to support the seamless transition of content across devices.

## Accessibility

Question:

What more could the Government and industry do to drive design and increase accessibility?

### Ofcom response

#### Audio-visual services

- 3.64 As the discussion paper noted, broadcasters have often exceeded the statutory targets applying to access services, particularly in relation to subtitling and audio description. At this stage, it is less clear how on-demand service providers will respond to the Government's objective of 'equivalence of access to communications services'. A report from ATVOD (the Authority for Television On Demand), due towards the end of this year, will shed more light on the extent of voluntary action by the industry.
- 3.65 In the related area of accessibility of electronic programme guides (EPGs), we agree that there have been promising developments in recent years, and consider that the maturity of text-to-speech technology offers scope for EPGs to be made much easier to use for consumers with visual impairments. As EPGs continue to evolve and provide greater utility to consumers, it will be important to ensure that, however they are delivered, they remain within the scope of regulation intended to promote and safeguard accessibility.

### Electronic communications services

- 3.66 Accessibility of electronic communications services is an important part of our current agenda on access and inclusion. Accessibility for these services currently is based on the concept of equivalence of access as set out in the Universal Service Directive. The Directive requires regulators to ensure that access and affordability in respect of Publicly Available Telephony Services is equivalent for disabled users as for the majority of end users. This establishes a requirement for equivalence under the EU regulatory framework for fixed voice telephony.
- 3.67 We recommend that the Communications Review considers whether a parallel requirement for equivalence to that set by the EU regulatory framework should extend to mobile and broadband services. Mobility and the ability to access the Internet and online services are increasingly important to ensure that no citizen or group of citizens is excluded from the benefits of electronic communications technologies and services. For some disabled users online accessibility is more important than for other users – for example because they are housebound and online is a convenient way to shop or to access medical or community services.

## Annex 1

# Lost and stolen mobile phones

- A1.1 In the last year we have carried out a review of the issue of unexpectedly high bills or 'bill shock'. We examined what causes bill shock and considered what more could be done by CPs, consumers and us to reduce the risk of it happening. We set out our findings and action plan in a statement in March 2012.<sup>22</sup>
- A1.2 One issue that we highlighted in our statement is the fact that consumers have unlimited liability for unauthorised use of their phones up to the point when they report their mobile phone as lost or stolen. This can cause unexpectedly high bills running to thousands of pounds if, for example, criminals make premium rate calls to particular numbers in order to get a share of the revenue. As part of our review we carried out a public call for inputs and the median bill reported by consumers who had experienced a lost or stolen mobile phone was £960. There have also been numerous stories in the media about consumers who have suffered bills of thousands of pounds after losing their phones or having them stolen.
- A1.3 The situation in the communications sector compares unfavourably with financial services, where liability for unauthorised financial transactions is capped at £50 (unless the consumer was complicit in the unauthorised use). This means that banks have a greater financial incentive than mobile operators to minimise consumer liability for unauthorised charges. We are encouraging mobile operators to do more to protect consumers generally by introducing and promoting more tariffs that allow consumers to set their own financial caps and receive usage alerts. But usage alerts alone will not help consumers who have experienced a lost or stolen phone as they will not receive the alerts. And not all consumers will be able to choose a tariff that enables them to set a financial cap or will exercise this choice if it is available to them. There might be a case, therefore, for the Government to consider introducing legislation to cap consumers' liability for the unauthorised use of lost/stolen mobile phones. In our view, it would be useful to explore:
- 1.3.1 whether the risk of loss as a result of unauthorised use of mobile phones is shared fairly between consumers and mobile operators; and
  - 1.3.2 what more should be done to protect consumers by, for example, reducing their liability or requiring operators to do more to alert them about unusual and potentially unauthorised use of their phones.

---

<sup>22</sup> <http://stakeholders.ofcom.org.uk/binaries/consultations/unexpectedly-high-bills/statement/statement.pdf>

**Annex 2**

# Smartphone security

## Maintaining a secure Smartphone Operating System

### Complexity

- A2.1 Contemporary Smartphone Operating Systems (OS) are highly complex. In 2008, the Android Smartphone OS consisted of around 11 million lines of code<sup>23</sup>. Security vulnerabilities within Smartphone OS and Apps are becoming commonplace and are exploitable by cyber criminals and unscrupulous individuals.
- A2.2 From a consumer perspective, it is arguably unclear who has the responsibility for the software security maintenance of the core Smartphone OS. Is it the OS vendor, handset manufacturer, the Mobile Network Operator (MNO), or a combination? Furthermore, it is commonplace for Smartphones to be configured and branded with particular MNO specified corporate branding and applications. MNOs adopt the latest versions of Smartphone OS at varying rates for new handsets. The fragmented nature of Smartphone OS may pose a further challenge to organisations/companies wishing to provide support to customers.

**Figure 1: Current distribution of Android versions**

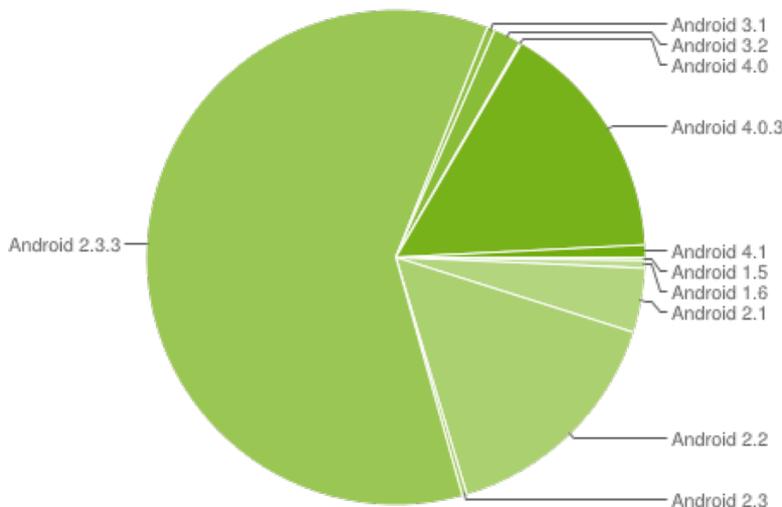


Image source: Google Play – Data collected up to 1<sup>st</sup> August 2012

<sup>23</sup> Google carves an Android path through open-source world | Underexposed – CNET News (22/05/2008). [http://news.cnet.com/8301-13580\\_3-9949793-39.html](http://news.cnet.com/8301-13580_3-9949793-39.html)

## Application market security

### App developer identity

A2.3 Consumers clearly benefit from a wide variety of Smartphone Apps. Such applications enhance the consumer experience of Smartphones allowing innovative services to emerge. Apps are available for purchase or free, downloaded from the OS vendor App marketplace. Handset OS vendor App marketplaces operate on a global basis, allowing developers to sell their applications to a worldwide market. The App developer's country of origin or identity of the App developer may be opaque to the end-user. Consumer concerns or feedback to the App developer may only be available via a freely available, disposable, web-based email address. App market refund policies differ, ranging from a 15-minute refund window to refunds available only for "faulty" Apps.

### App pre-release verification and remote removal

A2.4 Smartphone App marketplaces may test Apps prior to release into the marketplace. In the event of a submitted App being detected as behaving suspiciously or in a malicious manner the App will not be released into the market. The submission of a malicious application into a marketplace may lead to the termination of the App developer agreement for the developer concerned (i.e. breach terms of service). Even after release into the App marketplace, some OS vendors retain the capability to remove<sup>24</sup>, remotely, malicious Apps.

### Sideloaded Apps – trustworthy sources

A2.5 The sideloading of applications is the installation of an App via removable media, network, or third party website. This capability to sideload applications is not universal on all Smartphone handsets. Whilst sideloading may increase consumer choice and allow independent or niche development communities to emerge outside of the mainstream handset vendor marketplace, it may also expose the consumer to additional risks. Malicious fraudulent Apps, often-pirated versions of paid Apps, are in circulation on the internet and in particular available on file sharing web sites. Furthermore, we know of no capability to remotely disable or remove malicious Apps obtained from non-OS vendor market sources.

### Smartphone Rooting and Jailbreaking

A2.6 The Rooting or Jailbreaking<sup>25</sup> of a Smartphone OS allow the consumer to further configure and install non-approved applications. However, the act of Rooting/Jailbreaking can render the manufacturer warranty void and disbar the handset from receiving software updates thus further exposing the consumer to malware<sup>26,27</sup>. We have no data available to determine the extent of Rooted and Jailbroken handsets connecting UK mobile networks.

---

<sup>24</sup> Android Developers Blog: Exercising Our Remote Application Removal Feature: (23/06/2010). <http://android-developers.blogspot.co.uk/2010/06/exercising-our-remote-application.html>

<sup>25</sup> The term Root relates to the system super user root. Root has the highest privileges within a UNIX like operating system. Similarly the term Jailbreak relates to the UNIX term "jail" i.e. constrained system privileges

<sup>26</sup> Apple – Unauthorized modification of iOS has been a major source of instability, disruption of services, and other issues (27/09/2010). <http://support.apple.com/kb/HT3743>

## Security of mobile payments

- A2.7 Near Field Communications (NFC) utilises radio technology and licence exempt radio spectrum and operates typically over short distances. We are not currently aware of any vulnerability to the security of NFC based mobile payments at Electronic Point of Sale (EPOS) e.g. *the eavesdropping between the EPOS equipment and the Smartphone handset*.
- A2.8 However, we believe it is reasonable to consider that the security and integrity of mobile payments may be susceptible to compromise via the exploitation of handset OS and wider software vulnerabilities or the compromise of software-based cryptography. We note reports of a Smartphone App designed to capture NFC enabled credit card details over the air<sup>28</sup>.
- A2.9 The advent of peer-to-peer (P2P) payment Apps presents further challenges, allowing the electronic transfer of payments between individuals as opposed to retail merchants. It is conceivable that P2P payment apps will be of interest to organised cyber-criminals.

## Future risks

### Software based Subscriber Identity Module

- A2.10 The emergence of software based Subscriber Identity Modules (SIMs) offers the prospect of consumers switching between mobile networks more readily without recourse to a store visit. However, the compromise of the wider Smartphone OS may lead to conditions that prevent calls or interrupt services i.e. a denial of service.
- A2.11 Software based SIMs may lead to an increase in “slamming” (the switching of a phone contract without consent). We understand the proposed ability to change between mobile network provider is largely automated and requires less end-user invention (i.e. changing SIM cards) than conventional mobile carrier switching.

### Implications of 4G hi-speed connections

- A2.12 The advent of 4G services offers consumers with high-speed Internet connectivity comparable to that of today’s fast fixed Internet connections. As Smartphones and 4G become ubiquitous, it is likely that similar security issues and threats that have plagued the PC era will to some extent affect the Smartphone era e.g. BotNet Zombies, Denial of service, spam, Phishing, and extortion.
- A2.13 The theoretical Internet speeds available on 4G connections may make 4G an attractive platform for the mass infringement of copyright material. We note that file sharing Apps are available for Smartphones.

---

<sup>27</sup> Android Botnet Exploits Gingerbread Root Access – Security – Mobile Security – Informationweek: (09/02/2012). <http://www.informationweek.com/security/mobile/android-botnet-exploits-gingerbread-root/232600576>

<sup>28</sup> Symantec Ecardgrabber: Android App Sniffing Contactless Credit Card Details over the Air | Symantec Connect Community – (25/06/2012). <http://www.symantec.com/connect/blogs/ecardgrabber-android-app-sniffing-contactless-credit-card-details-over-air>