

FOREWORD

In 2009, the OECD Committee on Consumer Policy launched a review of the organisation's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce*. As part of the review, the committee developed an analytic report examining the consumer benefits and challenges in the acquisition of intangible digital content products. Based on the analysis, the committee developed this policy guidance, which it adopted on 15 September 2014, and recommended that it be made available to the public.

Note to Delegations:

This document is also available on OLIS under reference code DSTI/CP(2013)1/FINAL.

© OECD 2014

Applications for permission to reproduce or translate all or part of this material should be made to:
OECD Publications, 2 rue André-Pascal, 75775 Paris, Cedex 16, France; e-mail: rights@oecd.org

TABLE OF CONTENTS

I. Introduction.....	4
II. Scope.....	6
III. Consumer policy issues.....	7
A. Digital content product acquisition, access and usage conditions.....	7
Overview	7
Issue: Conditions of acquisition, access and usage	7
B. Privacy and security	9
Overview	9
Issue: Permission to collect, use and share personal data	11
C. Fraudulent, misleading and unfair commercial practices.....	12
Overview	12
Issue 1: Product changes, removal and liability when products do not perform as described or are defective	13
Issue 2: Unexpected charges and trial periods	13
Issue 3: Renewable contracts, renewable subscriptions and repeat purchases.....	14
D. Children.....	15
Overview	15
Issue: Advertising to children and education and awareness	16
E. Dispute resolution and redress	17
Overview	17
Issue 1: Identifying the source of access and usage problems	18
Issue 2: Consumer remedies.....	18
F. Digital competence.....	19
Overview	19
Issue: Enhancing consumer digital competence.....	20
REFERENCES	21

CONSUMER POLICY GUIDANCE ON INTANGIBLE DIGITAL CONTENT PRODUCTS

I. Introduction

In 2011, as part of an overall review of the OECD's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce* (OECD, 1999) (hereafter, "the 1999 e-commerce guidelines"), the Committee on Consumer Policy (hereafter, "CCP") launched analytical work examining trends and consumer policy challenges in the acquisition and use of digital content products, focusing on those that consumers store, access or receive in an electronic (i.e. intangible) format. Governments and other stakeholders (including businesses, civil society and academia) discussed a broad range of such issues at a roundtable and a workshop, which were held, respectively, in April 2011 (OECD, 2011*a*), and April 2012 (OECD, 2012*a*). Drawing on these discussions and independent research, a background report was developed by the CCP (OECD, 2013*a*). The analysis indicates that developments in the markets for intangible digital content products have been driven by a number of factors. These include:

- Expansion of Internet use and high-speed broadband capacity, which has provided a growing customer base and enhanced accessibility to the products.
- Continued innovation and enhanced competition, which have provided consumers with offers for a wider range of products, at competitive prices.
- More convenient and easy-to-use e-commerce payment mechanisms, which have simplified consumer acquisition of products.
- Growing use of mobile devices and applications (hereafter, "apps"), which is transforming the ways in which consumers shop, access and use the products.
- Development of cloud computing, which enhances the ability of businesses to offer services that allow consumers to acquire, organise, store, access and use the products, from anywhere and at any time.

The expansion of markets for intangible digital content products has been supported by the development of a number of channels that enable consumers to acquire and use content. These include traditional retail websites, online e-commerce platforms through which third party vendor products may be sold, Internet Protocol (IP) TV, and, increasingly, social media platforms.

Consumer complaints and surveys, however, reveal a number of challenges for consumers in acquiring and using intangible digital content products. These include:

- Inadequate information disclosure.
- Misleading or unfair commercial practices.

- Concerns about the collection, usage and sharing of consumer personal data.
- Inadequate dispute resolution and redress mechanisms; and
- Concerns about unauthorised charges associated with consumer usage of apps and online games.

This guidance provides a set of policy principles for addressing these issues. In developing it, the committee kept in mind the need to support innovation and the growth and dissemination of intangible digital content products. In light of the rapid development of markets for these products and information and communications technology (hereafter, “ICT”), the committee endeavoured to provide guidance that is technologically neutral.

In preparing the guidance, the committee built on the principles contained in the 1999 e-commerce guidelines and related policy instruments, which are as follows:

- *OECD Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* (OECD, 2002) (hereafter, “the 2002 security guidelines”).
- *OECD Recommendation of the Council Concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (OECD, 2003) (hereafter, “the 2003 cross-border fraud guidelines”).
- *OECD Recommendation of the Council on Consumer Dispute Resolution and Redress* (OECD, 2007a) (hereafter, “the 2007 recommendation on dispute resolution and redress”).
- *OECD Recommendation of the Council on Electronic Authentication* (OECD, 2007b) (hereafter, “the 2007 recommendation on electronic authentication”).
- *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce* (OECD, 2008) (hereafter, “the 2008 mobile commerce guidance”).
- *Consumer Education: Policy Recommendations of the OECD’s Committee on Consumer Policy* (OECD, 2009) (hereafter, “the 2009 recommendations on consumer education”).
- *Communiqué on Principles for Internet-Policy Making* (OECD, 2011b) (hereafter, “the 2011 OECD Communiqué”); and *OECD Recommendation on Principles for Internet Policy-Making* (OECD, 2011c).
- *OECD Recommendation of the Council on the Protection of Children Online* (OECD, 2012b) (hereafter, “the OECD 2012 Children Recommendation”).
- *OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD 2013b) (hereafter, “the privacy guidelines”); and
- *Policy Guidance on Mobile and Online Payments* (OECD, 2014).

The guidance reflects longstanding consumer protection principles in more traditional forms of commerce and comports with the core principle of the 1999 e-commerce guidelines that “consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce” (OECD, 1999, Part One).

II. Scope

This guidance covers intangible digital content products¹ (hereafter, “digital content products”) that are acquired on Internet platforms and mobile networks, and that are:

- Received in an electronic format (i.e. not acquired in a tangible form, such as on a CD), and
- Acquired by consumers from businesses *via* e-commerce (i.e. where the confirmation of product orders is carried out electronically), whether or not a monetary payment is involved.

The scope covers a broad range of digital content products, including media and entertainment items (such as film, music, games, virtual world items, literature, e-books, magazines, journals, images, news and IP TV services), apps and personalisation services/add-ons, including ringtones and screensavers. Such products, which are usually subject to licensing agreements, are generally delivered in an environment where the consumer’s experience is affected by different actors’ terms and conditions. In addition to digital content products providers, such actors may include, for example, the device manufacturers, operating system providers, mobile network operators and/or the providers of the platform where an acquisition is made and where the product is used. In some cases, these actors are digital content products providers, and, in other cases, they are not.

The policy principles in this guidance focus on the advertising and the terms and conditions that apply to consumers’ interactions related to the acquisition and use of digital content products, irrespective of the platforms through which the products are delivered by businesses and accessed by consumers. Such platforms include webhosting, e-mail and social networking, virtual world and cloud-based platforms. While the operators of these platforms are not the primary subject of this guidance, they may, however, be subject to certain principles in the guidance, to the extent that they are actively involved in the creation or control of advertising and marketing of digital content products.

Likewise, the policy principles may apply to those circumstances where the digital content products are sold in combination (i.e. bundled) with other goods and services. This can be beneficial to consumers, but may also raise challenges in determining the source of problems when such problems arise. A provider may, for example, offer a package that includes a broadband subscription, TV programmes (along with the possibility to store selected programmes), a video rental service and selected pay-TV channels *via* IP TV. Such packages could also include tangible products, such as recording devices.

Finally, it should be noted that some of the policy principles in this guidance do not apply equally to all types of transactions involving digital content products. As noted in section E of this guidance on dispute resolution and redress, for example, the types of remedies available for products which involve monetary payments may differ from those available for products for which no monetary payment is involved. Refunds, for example, would not apply to acquisitions where no monetary payments are involved; in such cases, other forms of redress (such as product replacement) may be afforded to consumers.

¹ The treatment of intangible digital content products differs among countries. Such products have been treated, for example, as goods, services, “mixed products” or as *sui generis* items. In some jurisdictions, the legal characterisation has not yet been established.

III. Consumer policy issues

The 1999 e-commerce guidelines provide basic principles on business and product information disclosures, advertising and marketing practices, dispute resolution and redress, payments, privacy, as well as education and awareness. They do not, as such, address the specific challenges arising from access and use of digital content products.

This guidance aims to complement the 1999 e-commerce guidelines. It covers issues concerning *a*) digital content product access and usage conditions, *b*) privacy and security, *c*) fraudulent, misleading and unfair commercial practices, *d*) children, *e*) dispute resolution and redress, and *f*) digital competence. A common issue in all these areas concerns the adequacy of information disclosures.

A. Digital content product acquisition, access and usage conditions

Overview

The 1999 e-commerce guidelines call on businesses engaged in e-commerce to provide sufficient information about the products being offered and the terms, conditions and costs associated with purchasing them, so as to enable consumers to make informed decisions (OECD, 1999, Part Two, Section III, C). The section recommends that:

“Such information should be clear, accurate, easily accessible and provided in a manner that gives consumers an adequate opportunity for review before entering into a transaction.”

“Businesses should provide consumers with a clear and full text of the relevant terms and conditions of the transaction in a manner that makes it possible for consumers to access and maintain an adequate record of such information.”

The guidelines further provide that “where applicable and appropriate given the transaction, such information should include ... details of and conditions related to withdrawal ...” (OECD, 1999, Part Two, Section III, C, *viii*). The 2008 mobile commerce guidance further suggests that businesses might provide consumers “with an opportunity, in mobile transactions, to withdraw from the transaction process until such time as they had had an opportunity to review the full contract and express an informed and deliberate consent to a purchase” (OECD, 2008, Section II). The suggestion was made in the context of a hypothetical example involving a consumer who accepts an offer for a “free” product *via* short message services without noticing contract terms appearing on the bottom of the page.

The above policy principles apply in principle to all types of products acquired *via* e-commerce. This guidance addresses the specific problems that may arise with digital content products.

Issue: Conditions of acquisition, access and usage

Technological advances are providing consumers with many new possibilities to copy, share, transform (from one format to another, for example) and transfer a wide range of digital content products. The ability of consumers to do so is usually governed by copyright laws, as well as the terms and conditions in end-user licensing agreements (hereafter, “EULAs”) and other terms of service, which may provide additional limits beyond those specified by copyright laws. Consumer access to and use of digital content products may also be affected by the presence of technological measures.

Limitations on the acquisition and usage of such digital content products can vary, sometimes significantly, from one product to another; furthermore, limitations on similar products may also exist across different service providers. For example, the period over which a consumer may be able to use a

product may be limited, or indefinite; copying beyond private use may or may not be permitted; the number of times a product (such as a piece of music or an e-book) can be accessed, streamed or downloaded may be limited; and there may be conditions or limitations on sharing a product with other parties (functionality limitations). Moreover, consumers may not always be able to access a product that they have lawfully acquired in one jurisdiction while travelling in another; they may be unable to acquire a digital content product offered by businesses located in other jurisdictions (geographical limitations). Further, consumers may be unable to play, listen to, or watch a product on different devices (interoperability limitations).

Some surveys reveal that consumers are often not aware of these limitations. Some digital content products providers do not disclose material information to consumers in a clear, conspicuous and unavoidable manner; some may not advertise their products in a manner that is consistent with product functionality, geographical and interoperability limitations. Moreover, the terms and conditions included in EULAs and terms of service provisions are, in many instances, long, complex and not easily accessible. In this respect, surveys carried out in a number of European Union Member States show that consumers often do not, or only partially, read these terms and conditions and may not understand what their rights and obligations are.

Both consumers and businesses could benefit from guidance on the types of information that should be provided to consumers on product access and usage conditions; such information should, in particular, point out any limitations to access and usage that may be included in EULAs and/or result from use of any technological measures. The guidance should also address ways in which such information should be presented to consumers (as, for example, provided in the EU's *Consumer Rights Directive*).²

Guidance

To help ensure that consumers are sufficiently aware of digital content product acquisition, access and usage conditions:

- i. *In the case where digital content products are offered on terms that are more restrictive than those that apply to tangible formats, the consumer should, where the terms are not self-evident, be clearly and conspicuously informed about them.*
- ii. *Businesses should provide consumers with information on the conditions for acquisition, access and usage of a digital content product early in the transaction process, in a clear, conspicuous and unavoidable manner.*
 - *Information should be presented in formats that can be easily read on different types of devices. In particular, stakeholders should work together to identify effective ways to provide consumers with information when the consumers are using mobile devices in an “on the go” context.*
 - *Information should include general and specific conditions regarding acquisition, access and usage of the products, in particular those which are not self-evident, such as:*
 - *Any limitations on the extent to which the product can be shared with other parties.*

² See http://ec.europa.eu/justice/consumer-marketing/files/crd_guidance_en.pdf.

- *Any limitations on the extent to which the product can be copied for personal use.*
 - *Any limitations on the type or number of devices or applications that can be used to access and use the product.*
 - *Any unexpected conditions under which a product or product access and usage could be modified by businesses following lawful acquisition by consumers.*
 - *Any limitations on accessing a product in different jurisdictions.*
 - *Any technical measures that have been put in place, including any effects that these measures may have on product or device usage.*
 - *Dispute resolution options.*
 - *Withdrawal rights (sometimes referred to as “cooling off” periods) and applicable refund, return, product replacement or repair options.*
- iii. *Businesses should ensure that their advertising for digital content products is not inconsistent with product usage and access conditions. They should provide consumers with summaries of the key terms and conditions governing the acquisition and usage of digital content products in a clear, conspicuous and unavoidable manner prior to consumers’ acquisition of such products. Stakeholders should work together to develop effective approaches for conveying such information to consumers.*

B. Privacy and security

Overview

The 1999 e-commerce guidelines (OECD, 1999, Part Two, Section VII) indicate that e-commerce should be conducted “in accordance with the principles of the OECD’s privacy guidelines”, which were adopted in 1980 and revised in 2013 (OECD, 2013*b*). The guidelines contain eight basic principles of domestic application that address the collection and use of personal data (Box 1).

Box 1. OECD Privacy Guidelines' Eight Basic Principles (OECD, 2013b)

Collection Limitation Principle. There should be limits to the collection of personal data; such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for these purposes should be accurate, complete and kept up-to-date.

Purpose Specification Principle. The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the preceding paragraph] except a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle. Individuals should have the right a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

The above principles were supplemented in 2013 by new provisions on implementation and global interoperability. The new provisions provide that a data controller should:

“Have in place a privacy management programme that provides for appropriate safeguards based on privacy risk assessment.”

“Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects” (OECD, 2013b, Part III, respectively paragraph 15a *iii* and c).

In addition to these principles, issues relating to privacy and security are also addressed in the 2008 policy guidance on mobile commerce (OECD, 2008). These largely concern location-based information tracking of consumer activities in mobile commerce. Security issues are also addressed in the OECD's 2002 security guidelines (OECD, 2002) and the OECD's 2007 recommendation on electronic authentication (OECD, 2007b).

This guidance complements the above principles, focusing on the specific context of the acquisition and use, by consumers, of digital content products.

Issue: Permission to collect, use and share personal data

Many different entities typically have access to the personal data that is provided by consumers when they acquire products *via* e-commerce. In addition to payment providers and merchants, operating system platform providers, hardware manufacturers, mobile operators, content and application developers, data analytics companies, advertisers and coupon and loyalty program administrators may have access to such data. Such access and use, by businesses, of personal data can be beneficial for consumers. Its use for commercial purposes, such as targeted marketing, for example, can help consumers to discover products which might be of interest. In some cases, commercial use of consumer data by businesses enables them to provide consumers with products for “free” (i.e. with no monetary payment) or at discounted prices. Moreover, such data can help to reduce fraud (by improving authentication), which benefits both consumers and businesses.

In the case of digital content products, additional personal data is often collected following the acquisition, when the products are being used by consumers. This data may be provided by the consumer voluntarily or it may be observed and acquired by businesses, sometimes without consumer knowledge or consent. This would be the case, for example, when an app provider accesses geo-location data, and/or IP addresses. In many instances, such data is necessary for the product to run or to be updated. This is common, for example, for apps that provide location-based services on mobile devices.

Businesses’ collection, use and sharing of consumer data with third parties may raise privacy concerns for consumers:

- Information on the collection, use or sharing of consumer data may not be available to consumers prior to the acquisition of the digital content product. In the case of apps, information on the type of consumer data required to download or use the app may not be available or accessible even after the product is acquired. Moreover, it may not be possible for consumers to alter the permissions that they may have granted prior to acquiring the app.
- Information about the collection, use or sharing of consumer data that is unrelated to the transaction involving a digital content product may not be adequately provided to consumers. For example, some e-book providers are able to collect data about their customers’ reading behaviour for purposes other than improving the customer’s reading experience, sometimes without consumer knowledge and/or consent.
- Consumers may not want their activities being followed (i.e. tracked) and their data being used or shared with third parties for commercial or other purposes. Such tracking and monitoring, which can be easily conducted through the use of cookies and via cloud-based product storage and streaming services, enable companies to get insights into consumer behaviour, including what consumers search for, read, highlight, comment on, listen to, share with, and with whom, when and for how long. Such information can, for example, be gleaned from e-books without the knowledge of the reader (OECD, 2012c).

Guidance

To help ensure transparency, choice and control in the collection and use of personal data:

- i. *Businesses should provide consumers with clear and conspicuous information about the collection and use of their personal data, and the measures that consumers can take to manage such data.*

- *Prior to the acquisition of a digital content product, consumers should be provided with clear and conspicuous notice of the types of personal data that will be collected about them and used by businesses, when acquiring and while using a digital content product.*
 - *Consumers should be provided with clear and conspicuous information on the ways in which they can set and manage the privacy settings (or permissions) linked with a digital content product. They should also be able to easily review the permissions they have granted to businesses.*
- ii. *Businesses that collect and use personal data other than that which is legally required or necessary to complete a transaction or to use a digital content product or for an update of such product, should provide consumers with appropriate choice mechanisms to allow them to limit or deny the collection and use of such data.*
 - iii. *Businesses should obtain express consent before collecting and using sensitive data, such as individualised geo-location data, health information or financial information.*
 - iv. *Businesses should be mindful of the risks, both to themselves and to consumers, associated with the over-collection of personal data, particularly the risks of data being stolen, lost or misused by third parties.*
 - v. *Businesses should delete personal data that is collected when consumers acquire and use digital content products when they no longer need such data.*
 - vi. *Businesses should put in place appropriate safeguards to give effect to the above privacy principles when they design and develop digital content products. Such safeguards should apply equally to products which involve monetary payments and to those which do not. Businesses are encouraged to work with other stakeholders on the development and design of these privacy safeguards.*

C. Fraudulent, misleading and unfair commercial practices

Overview

The 1999 e-commerce guidelines call on businesses engaged in e-commerce to pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices (OECD, 1999, Part Two, Section II). Businesses are: *a)* called on not to make any representation or omission or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair (OECD, 1999, Part Two, Section II) and *b)* encouraged to establish limitation of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms (OECD, 1999, Part Two, Section V). In addition, governments are called on to co-operate at the international level to combat cross-border fraudulent, misleading and unfair commercial conduct, through information exchange, co-ordination, communication and joint action.

The 2003 cross-border fraud guidelines provide further guidance with respect to government policies. These guidelines encourage “governments to put frameworks in place that would help limit, prevent and deter fraudulent and deceptive commercial practices involving business and individuals”. In particular, the guidelines state that OECD members should provide for effective mechanisms to “adequately investigate,

preserve, obtain and share relevant information and evidence relating to occurrences of fraudulent and deceptive commercial practices”, “stop businesses and individuals engaged in fraudulent and deceptive commercial practices” and “provide redress for consumer victims of fraudulent and deceptive commercial practices” (OECD, 2003, Section II, A 2, 3 and 4).

This guidance aims to complement the above principles, focusing on those issue areas where consumer problems and legal gaps and uncertainties have been reported in a number of jurisdictions. These issue areas concern consumer problems associated with *i*) material changes to the products’ nature or availability, product removal, and liability when such products do not perform as described or are defective; *ii*) unexpected charges and trial periods; and *iii*) renewable contracts, renewable subscriptions and repeat purchases.

Issue 1: Product changes, removal and liability when products do not perform as described or are defective

The background report on digital content products identified various practices that may constitute fraudulent, misleading and unfair commercial practices in some jurisdictions. These include: businesses’ failure to provide key information about provisions limiting businesses’ liability in the case of problems related to the non-performance of an acquired product; product updates by businesses that have affected consumer usage adversely; changes in the availability of a product without prior notification to consumers; and lack of redress in the case of defective products.

Guidance

To help protect consumers from fraudulent, misleading and unfair commercial practices:

- i. Businesses should provide consumers with remedies for the digital content products that they have lawfully acquired that do not perform as advertised, described or that are defective. Such remedies:

 - *Could include repair, replacement or reimbursement.*
 - *May be available for an appropriate period of time (which may be limited in some cases) after the acquisition of the product, taking technological developments that may affect use of the product into account.**
- ii. Businesses should inform consumers of any material changes or updates to the products that they have lawfully acquired and that would adversely affect their access to or use of such products.*
- iii. Consumers should be notified of any material changes to the accessibility of a product that they have lawfully acquired; they should be provided with appropriate redress in the event of any detriment arising from such changes.*

Issue 2: Unexpected charges and trial periods

When acquiring or using digital content products, consumers sometimes incur charges that they did not authorise; they are also sometimes charged for products that they thought were free or did not knowingly purchase. Complaints have been made, for example, about fees for products being charged automatically after a trial service period had ended, without consumers having received sufficient notification. Consumers have in particular reported concerns about charges associated with mobile apps

that they have acquired for “free”. In such instances, consumers were sometimes unaware that additional charges would be applied when certain premium features were used, or the apps were used to make purchases (i.e. “in-app” purchases).

Guidance

To help protect consumers from unexpected charges that could result when trial periods have lapsed or when use of a digital content product results in new charges:

- i. If the use or acquisition of a digital content product results in a charge, consumers should be so informed and their express consent for such charges should be obtained.*
- ii. When digital content products are provided to consumers on favourable terms for a limited period of time (i.e. a trial period), information on the length of the trial period and the charges that will be incurred once the trial period has lapsed, should be provided clearly and conspicuously to consumers, early in the transaction process, as should information on the steps to be taken to discontinue purchasing the good or service (i.e. steps to be taken to discontinue the relationship either during or, where applicable, after the trial period).*
- iii. Consumer express consent should be obtained for continuing a commercial relationship beyond a trial period, before consumers pay or incur any additional financial charges.*

To help protect consumers from unexpected charges associated with use of digital content products, businesses and other stakeholders should work together to:

- i. Provide consumers with clear, conspicuous and unavoidable information on the costs that could be incurred in using a digital content product, particularly with respect to additional digital content products that may be acquired through, for example, in-app purchases.*
- ii. Obtain consumer express consent for any charges associated with the use of digital content products.*

Issue 3: Renewable contracts, renewable subscriptions and repeat purchases

When they are acquiring digital content products, consumers are sometimes not clearly informed that the terms and conditions contain provisions for automatic repeat purchases of products or automatic contract or subscription renewals. There have been instances where, for example, consumers purchasing software online were informed in their end-user licensing agreements that they would have the option to renew the agreement upon expiration; in practice, however, the agreement was renewed automatically, resulting in consumers being charged for products they may not have wanted. In other instances, consumers purchasing ringtones through their mobile phones did not realise that they had, at the same time, subscribed to an ongoing service.

Guidance

To help ensure that consumers are adequately informed about automatic repeat purchases as well as contract and subscription renewals:

- i. *Businesses should, early in the transaction process clearly and conspicuously inform consumers when their offers for digital content products and related products involve a repeat purchase or a renewable subscription, which require consumers to take steps to cancel a transaction (i.e. negative option billing); this should include disclosure of the amount and frequency of any recurring charges.*
- ii. *Consumers should be provided with easy-to-use procedures for preventing automatic renewals of contracts and for terminating recurring charges; such procedures should be communicated to them when a transaction is confirmed.*
- iii. *Unless they waive the option expressly, consumers should be notified when an automatic repeat purchase will be made or when a subscription will be automatically renewed. Notification should be made in a clear and conspicuous manner and sufficiently in advance to enable consumers to cancel the purchase or renewal; it should include information on how such cancellation may be made.*

D. Children

Overview

The 1999 e-commerce guidelines provide that:

“Advertising and marketing should be clearly identified as such.”

“Businesses should take special care in advertising or marketing that is targeted to children ... who may not have the capacity to fully understand the information with which they are presented” (OECD, 1999, Part Two, Section II).

The 2008 policy guidance on mobile commerce provides examples of situations where problems could arise when children who have access to mobile devices use them to purchase products without the knowledge or consent of their guardians, resulting, for example, in excessive or inappropriate purchases (OECD, 2008, Section III). The problems are notable in the case of mobile devices as purchases can often be made without a child having to provide any payment information, as such purchases may simply be added to the account of the mobile phone subscriber. To address this issue, the 2008 mobile commerce guidance provides that stakeholders could (OECD, 2008, Section III):

“Provide parents with the ability to set a ceiling that would limit the amount of charges that children could accrue when using mobile phones, by, for example, setting a limit on the number of text messages, or establishing monetary limits on downloadable purchases.

Encourage mobile devices to be designed in a way that users could limit the types of transactions.

Encourage mobile operators to send warnings/notices to parents when expenditures exceed an established ceiling level.”

The committee’s 2009 recommendations on consumer education further indicate that “it is important to educate parents along with their children about their responsibilities online, as well as the techniques that are frequently used online to market products” (OECD, 2009, Annex II).

The committee's 2014 policy guidance on mobile and online payments (OECD, 2014, Section E) provides that businesses, governments and other stakeholders should:

“Work together to provide parents and guardians, prior to the children's purchase of or access to goods or services that are likely to generate charges incurred by children, with clear, conspicuous and easily accessible information on the costs that may be incurred in acquiring, accessing or using goods and services, and information on how to avoid those costs.

Develop effective mechanisms to enable parents or guardians to ensure that payments initiated by children are subject to their authorisation.

Develop tools which enable parents or guardians to exercise different types of controls over the purchases they authorise their children to make; this would include, for example, tools to prevent children from making purchases without express parental consent or tools that enable parents or guardians to establish ceilings on the amounts that could be charged to an account during defined periods.

Inform parents or guardians about the availability of such tools in a clear and conspicuous manner.”

This guidance complements the above principles by addressing issues associated with advertising to children that is integrated into digital content products; it also provides recommendations to businesses and other stakeholders on ways in which parents, guardians and children should be educated and made aware of such advertising practices.

Issue: Advertising to children and education and awareness

Growing use by children of digital content products, such as apps and online games, can provide entertainment, as well as educative tools. However, while in most countries children generally do not have the legal capacity to make payment commitments, they have been able, in a number of instances, to acquire additional product features or content without their parents or guardians' knowledge or consent. Once, for example, children are using an app or an online game, they may be able to incur charges for additional content without always having to enter a password or financial information. The fact that some products may be advertised as “free” or without disclosure of possible additional charges could further complicate the situation as the account holder (commonly a parent or guardian) may not be aware that they or their children may incur charges for acquiring additional digital content products while using the products.

Although direct exhortations to children are prohibited in many OECD countries, there is concern in some countries that, while using digital content products, children may be prompted by commercial advertising that is integrated into the products. These advertisements may, for example, pop up in an animated form while a game is being played, using language, design and visual interfaces that are specifically designed to appeal to children. Moreover, there are concerns in some jurisdictions that children may sometimes be enticed into acquiring additional digital content products to, for example, enhance their performance while playing an online game in multi-user or social media environments. In such circumstances, children might not understand that acquiring such additional products would lead them to incur monetary charges on the account, without the account holder's knowledge and consent. In some countries, legislation and guidelines have been developed to prohibit such practices.

Guidance

To address concerns related to advertising targeted at children and to the possibility that children can incur monetary charges in connection with the acquisition and use of digital content products without the

knowledge and/or consent of their parents, guardians or account holder, businesses, governments and other stakeholders should:

- i. *Take special care that commercial advertising is presented in a way that is clearly identifiable as such, taking into account the likely ages of the children using the products.*
- ii. *Ensure that commercial advertising and other material describing the features of digital content products are not deceptive or misleading with respect to charges that may be incurred by children while using such products.*
- iii. *Educate parents and guardians about the situations in which children may be prompted to acquire additional digital content products while using a digital content product and raise their awareness of any commercial practices that are misleading or unfair under applicable law.*
- iv. *Develop similar education and awareness programmes aimed to sensitise children to situations where they might be exposed to advertising for acquiring additional digital content products while using a digital content product. Such programmes should take into account the likely ages of the children using the products.*

E. Dispute resolution and redress

Overview

The 1999 e-commerce guidelines call on businesses, consumer representatives and governments to work together to “continue to use and develop fair, effective and transparent self-regulatory and other policies and procedures, including alternative dispute resolution mechanisms, to address consumer complaints and to resolve consumer disputes ... , with special attention to cross-border transactions” (OECD, 1999, Part Two, Section VI, B).

The 2007 recommendation on dispute resolution and redress elaborates on this principle, establishing a framework for such procedures. The recommendation calls on governments to “encourage businesses and industry groups to provide consumers with voluntary mechanisms to informally, and at the earliest possible stages, resolve their disputes and obtain redress as appropriate” (OECD, 2007, Annex, Section IV, 1). The recommendation, for example, encourages payment card issuers to “provide consumers with remedies for disputes arising out of transactions for goods and services”; it suggests that “such protection may include, for example, limitations on liability to pay for non-delivered or non-conforming goods or services” (OECD, 2007, Annex, Section IV, 2.c).

In the 2011 OECD Communiqué, governments, businesses and the Internet technical community recognise that in order to build public trust in the Internet environment, policy-making processes and substantive policies that ensure transparency, fair process, and accountability should be encouraged. Transparency ensures that Internet users have timely, accessible, and actionable information that is relevant to their rights and interests. Fair process provides predictable decision-making procedures to govern the definition, assertion, and defence of rights. Accountability is achieved through policies that make parties answerable, where appropriate, for their actions on the Internet (OECD, 2011*b*). At the same time, the Communiqué recognises the fundamental role that appropriate limitations of liability for Internet intermediaries have, and continue to play, in particular with regard to third party content, in promoting innovation and creativity online. However, as the Communiqué also underscores, in addition to promoting economic growth, Internet intermediaries, like other stakeholders, can and do play an important role in

addressing and deterring illegal activity, fraud and misleading and unfair practices conducted over their networks and services (OECD, 2011*b*).

When faced with problems relating to access and usage of digital content products, consumers have reported difficulties in determining which, from the various parties involved in a transaction (such as the digital content provider, the developer, the platform operator, or, in some instances, the mobile network operator) they should contact to resolve a problem, and/or get redress. This guidance expands on the above principles to help businesses assist consumers in *i*) identifying the source of a problem affecting access and usage of a digital content product and, thereby, the relevant party whom they should turn to; and *ii*) obtaining the remedies that are to be available when such problem occurs.

Issue 1: Identifying the source of access and usage problems

The ability of consumers to identify the source of a quality problem encountered when accessing and using a digital content product is sometimes limited. Consumers may not always be able to determine whether the problem originates from the content itself, the device on which the digital content product is accessed or the service (such as the Internet service) that enables access to the product. Another area raising questions relates to the role that may be played by a digital platform (such as a cloud platform) on which digital content products are being sold by, or on behalf of a third party content provider. In such a complex environment, consumers may not know whom, from the content provider, the platform operator (such as an online retailer or a social networking website), or the provider of a communication service (such as an Internet service provider or a mobile network operator), to turn to, to resolve issues. Whether the platform operator is, for example, responsible for providing consumers with product and business-related information disclosures, is an issue being explored in some jurisdictions.

Guidance

To help clarify which parties consumers should turn to when they have a problem with access and usage of a digital content product:

- i. Businesses involved in a transaction should assist consumers in identifying the origin of a problem that materially and adversely affects a consumer's access and use of a digital content product. This would include helping consumers determine whether the problem originates from the platform enabling access to the product, the product itself, or the device on which the product is being used.*
- ii. Guidance should include clear information about the party to whom they should turn to resolve different types of problems and how that party could be contacted.*
- iii. If a problem is neither related to the device being used by a consumer, nor to the provider of the communication service, information on the extent to which responsibility for addressing the problem resides with the platform through which the product is lawfully acquired, or the content provider, should be clearly and conspicuously provided to the affected consumer.*

Issue 2: Consumer remedies

In most OECD countries, legal and private-sector voluntary remedies are often not applicable to digital content products, or the remedies may vary, depending, for example, on the way the digital content product is supplied to consumers (*via* streaming or download) and its treatment as a good, a service, or a *sui generis* product (OECD, 2012*a*; OECD, 2013*a*). Treatment as a service or a *sui generis* product, for

example, may affect the availability of certain consumer remedies, such as rights of withdrawal and/or the ability to return a product, obtain refunds, price reductions, or product exchange or replacement. The situation is further complicated when cross-border transactions take place and treatment differs between the jurisdictions involved.

Moreover, consumer remedies may vary depending on whether a monetary payment was made to acquire a product, or not. For example, in instances where a product acquired for “free” does not perform as expected or is defective, a refund would not be available. Other forms of redress may however be afforded to consumers, such as replacement of the digital content product or of any affected device, as appropriate.

Guidance

To provide consumers with adequate redress mechanisms when problems with access and use of digital content products arise:

- i. *Businesses should provide redress to consumers for the detriment that they suffer as a consequence of digital content products which are defective, damage their devices or do not meet advertised quality criteria.*
- ii. *Governments, businesses and other stakeholders should work together to identify the types of remedies that should be available to consumers when acquiring digital content products within or across borders if such products do not perform as expected or are defective. This could include repair or replacement of faulty content or, if this is not possible, rejection and compensation, including, as appropriate, full or partial refund.*
- iii. *Governments, businesses and other stakeholders should determine the type of redress that consumers may be entitled to in the case of problems with digital content products that have been lawfully acquired without any monetary payment. Consideration should be given in that regard to the type and level of detriment suffered by consumers.*
- iv. *Information on the availability of such remedies should be provided to consumers early in the transaction process in a clear and conspicuous manner.*

F. Digital competence

Overview

The 1999 e-commerce guidelines call on stakeholders to work together to “educate consumers about electronic commerce, to foster informed decision making by consumers participating in electronic commerce, and to increase business and consumer awareness of the consumer protection framework that applies to their online activities” (OECD, 1999, Part Two, Section VIII). The 2009 CCP recommendations on consumer education further underscore the importance of enhancing digital competence. In particular, the recommendations provide that consumers need to have knowledge of technology and media and be aware of their rights and responsibilities when engaging with digital media (OECD, 2009, Annex II). Likewise, the 2011 OECD Communiqué provides that “governments, the private sector, the Internet technical community and civil society should all work together to provide the capacity for appropriate and effective individual control over the receipt of information and disclosure of personal data, which should include user education and digital literacy initiatives” (OECD, 2011b).

The importance of education and digital skills is also reflected in the OECD 2012 Children Recommendation (OECD, 2012*b*), which states that “governments should foster awareness raising and education as essential tools for empowering parents and children, by, for example:

- Integrating Internet literacy and skills in school curricula with a focus on risks and appropriate online behaviour;
- Training educators and encouraging other stakeholders to educate and raise awareness of children and parents;
- Regularly measuring the evolution of their Internet literacy.”

Building on the above principles, this guidance calls for the development of education and awareness programmes that would provide consumers with up to date knowledge and skills to acquire and use digital content products in a safe and responsible manner.

Issue: Enhancing consumer digital competence

The level of consumer knowledge and skills with digital technology and media can vary within and across countries depending on gender, age and social background. In addition to knowing what their rights, obligations and responsibilities are, consumers need to be provided with adequate skills on ways that digital content products can be used safely and in a responsible manner. With respect to the latter, consumers often have, for example, insufficient knowledge of how copyright laws operate within and across jurisdictions in general, and how they might apply in particular instances. In addition to developing capacity in these areas, consumers also need to ensure that they keep up with and understand developments in the complex and rapidly changing digital content marketplace.

Guidance

To help enhance consumer digital competence in the acquisition and usage of digital content products:

- i. Governments, businesses and other stakeholders should work together to develop adequate education and awareness programmes aimed at providing consumers with the relevant knowledge and skills to acquire and use digital content products. In this regard:*
 - *Ways in which such programmes might be integrated into school curricula should be explored.*
 - *Efforts should be made to develop programmes which target the needs of different age groups.*
 - *Such education and awareness programmes should include opportunities for consumers to upgrade and update their skills. The programmes should themselves be reviewed periodically and adapted to the rapidly changing information and communication technology and digital content products environment.*
- ii. Such programmes should provide consumers with a means to enhance their knowledge of their legal rights and obligations. Special consideration should be given to enhancing consumer knowledge and awareness of the terms and conditions governing the use of copyrighted products.*

REFERENCES

- OECD (Organisation for Economic Co-operation and Development) (1999), *Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, Paris, 1999, www.oecd.org/dataoecd/18/13/34023235.pdf.
- OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks*, OECD, Paris, 2002, www.oecd.org/sti/ieconomy/15582260.pdf.
- OECD (2003), *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, Paris, www.oecd.org/sti/crossborderfraud.
- OECD (2007a), *OECD Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, 2007, www.oecd.org/dataoecd/43/50/38960101.pdf.
- OECD (2007b), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*, OECD, Paris, 2007, www.oecd.org/sti/ieconomy/38921342.pdf.
- OECD (2008), *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment issues in Mobile Commerce*, *OECD Digital Economy Papers*, No. 149, OECD Publishing, doi: [10.1787/230363687074](https://doi.org/10.1787/230363687074).
- OECD (2009), *Consumer Education, Policy Recommendations of the Committee on Consumer Policy*, OECD, Paris, October, www.oecd.org/dataoecd/32/61/44110333.pdf.
- OECD (2010), *Consumer Policy Toolkit*, OECD Publishing, doi: [10.1787/9789264079663-en](https://doi.org/10.1787/9789264079663-en).
- OECD (2011a), *OECD Roundtable on Consumer Protection in the Purchase of Digital Content Products: Summary of Discussion*, [http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=DSTI/CP\(2011\)14/FINAL&docLanguage=En](http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=DSTI/CP(2011)14/FINAL&docLanguage=En).
- OECD (2011b), *Communiqué on Principles for Internet Policy-Making*, OECD, 2011, www.oecd.org/internet/innovation/48289796.pdf.
- OECD (2011c), *OECD Council Recommendation on Principles for Internet Policy Making*, 13 December 2011, www.oecd.org/internet/ieconomy/49258588.pdf.
- OECD (2012a), *OECD Workshop on Consumer Protection and Empowerment in the Purchase of Digital Content*, <http://oecd.org/sti/consumerpolicy/oecdworkshoponconsumerprotectionandempowermentinthepurchaseofdigitalcontent.htm>.
- OECD (2012b), *Recommendation of the Council on the Protection of Children Online*, OECD, Paris, February 2012, <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>.
- OECD (2012c), *E-Books: Developments and Policy Considerations*, *OECD Digital Economy Papers*, No. 208, OECD Publishing, doi: [10.1787/5k912zxcg5svh-en](https://doi.org/10.1787/5k912zxcg5svh-en).

OECD (2013a), *Protecting and Empowering Consumers in the Purchase of Digital Content Products*, OECD Digital Economy Papers, No. 219, OECD Publishing, doi: [10.1787/5k49czlc7wd3-en](https://doi.org/10.1787/5k49czlc7wd3-en).

OECD (2013b), *Revised Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 2013, www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OECD (2014), *Consumer Policy Guidance on Mobile and Online Payments*, OECD Digital Economy Paper 236, OECD Publishing, doi: [10.1787/5jz432cl1ns7-en](https://doi.org/10.1787/5jz432cl1ns7-en).