Rivista Italiana di Antitrust
Italian Antitrust Review
N. 1 (2015)
Articles

CONSUMER LEGISLATION AND E-COMMERCE CHALLENGES

Jason Freeman[1]

Keywords: consumer protection, e-commerce, European Union, unfair commercial practices directive, enforcement

Abstract: *Where there is vigorous competition, and consumer confidence, there is economic growth. E-commerce drives both of these but there remain situations where traders exploit technology or consumer behavioural biases, and seek to compete on the wrong things –such as unrealistic up front prices. This harms competition and can reduce consumer trust, meaning that consumers consume less. This could occur when traders: i) prevent consumers from accessing, assessing or acting on information, and so make the wrong choice; ii) take advantage of their superior understanding of technology to collect data or money from consumers; iii) abuse the advantages of the internet (ease of set up, cross jurisdictional reach, access to markets) to misrepresent the price, the quality, the range of products on offer, or the service you will get.*

Firms should therefore behave responsibly, and not seek to steal an unfair march on their competitors. Effective enforcement incentivises the right behaviours.

In order to enforce effectively, EU agencies need to prioritise robustly and build strong competence in internet investigation. Increasingly enforcement activities need to be run as international projects involving non EU enforcers and industry allies –and we need to be willing to protect overseas consumers as well as our own.

It is important that the legal framework facilitates, rather than hinders, enforcement –so that for example investigators can easily discover the true identity of traders who run anonymous websites, that they are able to carry out covert test purchases, and so that websites causing harm to the economic interests of consumers can swiftly be removed.

There are a number of areas where the EU legislator should consider further work, in order to address those persistent threats that have proven difficult to eradicate so far: clarifying the scope of platform responsibility; extending consumer protection to all individuals; ensuring all CPC enforcers have clear robust evidence gathering powers; providing a straightforward and cheap website take down power; ensuring enforcers are able protect non EU consumers, and can secure redress.

1. INTRODUCTION

E-Commerce is an opportunity for economic growth in the EU. However there are barriers to the full realisation of its potential. These are both traditional obstacles to competition and problems that are specific to e-commerce - where the distinctive benefits that e-commerce brings are subverted. There are several ways to overcome these barriers - and effective enforcement is one of them. So I will also consider some of the areas where current consumer legislation could be improved in order not to hinder enforcement.

[1] Director, Consumer Law, Competition and Markets Authority, UK.

2. WHAT DRIVES GROWTH?

Vigorous competition plus consumer confidence equals economic growth. Competition gives firms incentives to deliver what consumers want as efficiently and innovatively as possible – so that they strive to cut prices, and improve product quality and range, and service. Confident, well informed and rational consumers drive firms by effectively shopping around, rewarding those firms that offer the best deal. Problems arise when firms exploit technology or consumer behavioural biases, to prevent consumers from accessing, assessing, or acting on key information, or the structure of the market is such that competition does not work well. The question then is whether enforcement can correct these problems.

The point of enforcing consumer rights online is to drive competition and ultimately economic growth. Consumer law ensures a level playing field for traders – and ensures that they don't compete on the wrong things, such as fake headline prices, technological trickery or concealed terms and conditions. Where businesses behave badly, products don't improve and prices are high, the wrong firms survive, and consumer choice is harmed, and ultimately consumer trust is eroded, leading to reduced consumption. Where enforcement is effective it disciplines traders through having a deterrence effect, and encourages consumers by building trust. However businesses also need to take responsibility for the growth of the economy by treating customers fairly, rather than exploitatively. Badly behaved businesses may face punishment in the form of enforcement action and failure, if sufficient consumers switch, but there is a need for commercial morality, without which the market is not able to reach its full potential, due to a deficit of consumer trust and engagement.

3. BARRIERS TO EFFECTIVE COMPETITION

Firms know that consumers have behavioural biases, and they may exploit these in order to distract consumers from their task of making effective choices. Firms sometimes prevent consumers from *accessing information*, for instance by concealing their terms and conditions, or making them very onerous to read, and by making it hard to identify the actual price (perhaps by concealing compulsory price components until late in the purchasing process). They also prevent consumers from *assessing information*. Prices or key terms may be overly complex, so that it is hard to compare. Prices may be partitioned, or compared to spurious reference prices, so that it is more difficult to calculate actual value. Sometimes the consumer is distracted by the way the information is presented, for instance where attractive headline claims are qualified by an asterisk, or they are simply given too much choice (information overload). Finally firms may try to stop consumers from *acting on information*. This may be by contract terms that impose high charges for unexpected purchases, or impose barriers to switching. Or it may be making the switching process unnecessarily difficult – such as when a continuous payment authority, which it is easy to sign up to online,

requires the consumer to phone a particular number (and then be kept on hold for a long time, before being hard sold some other option) to terminate.

Firms also have the upper hand when it comes to technology. Most consumers are unaware of the way their computer or smart phone actually operates, whereas businesses invest heavily in tech development. This leads to a blind spot, where competition between firms does not occur. For example, where an online service is ostensibly "free", but in fact uses cookies or other technological means, over which the consumer has limited control, to collect data, there is unlikely to be competition between traders on the level of data that is collected – the "price" for using the service. Likewise, where a consumer downloads an app, the permissions may involve extensive data collection – yet the consumer may be essentially unaware of what is being harvested. Nor are they able to make an effective choice, since they cannot distinguish easily between the permissions that are necessary for the effective functioning of the app, and those that are collecting data as part of the monetisation plan that the trader has.

The difficulties that the consumer may face are arguably worse when actual money is involved. The link between a device and a payment mechanism brings considerable convenience benefits, smoothing transactions. However when the consumer does not know that the settings actually open a "payment window" during which no authorisation code need be entered, and especially where the fact of making a payment is not made clear in an app (such as when, during a game, the consumer is exhorted to "upgrade now" or similar, when in fact this is a step that requires payment), the scene is set for consumers to run up large, unwanted bills, and for those businesses that are least transparent to gain an unfair competitive advantage over their rivals. A similar problem arises from practices around continuous payment authorities or "negative options", when the trader unfairly infers consent to take more money from the consumer's payment account, by the use of hidden terms, or misleading "free trial" claims.

From enforcement experience, it is possible to identify many instances where businesses seek to subvert effective competition on price, range, quality and service. Drip pricing often occurs when there is intense competition on prices – so that firms have an incentive to present an artificially low up front price, and then recover additional sums through later add ons, whether they are last minute surprises or spurious optional extras, that are added during the click through process. Consumers have a tendency to focus on the headline price, and then overpay for the additional extras, meaning that the least transparent business derives most profit! This is therefore an area where there has been enforcement pressure to change.

The online market – due to the fact that goods are only displayed virtually, and the trader is not physically present- makes it relatively easier for businesses to claim, falsely, that they have an impressive range of products, when in fact they do not. For example in the case of resale of tickets for the 2012 London Olympic Games, the OFT found that several websites had taken orders for many more tickets than they were actually able to supply at the time of

order. Similarly, the online seller of electrical goods, Shop4Tek, took orders and then failed to deliver. These practices are problematic, because it is more efficient for consumers to shop online – they should have more range, at potentially lower prices, than shopping locally. However where range is misrepresented in some way, this damages consumer trust.

Firms rightly compete on quality, and online reviews enable consumers to judge this more accurately up front. However the phenomenon of fake reviews (where positive reviews are purchased for money, negative reviews are removed, or reviewers act in bad faith) threatens to devalue this important information source.

These examples show that the internet, though an undoubted force for economic growth, presents some inherent weaknesses, which could be said to be the flip side to its great strengths. The internet has revolutionised Europe's economy by providing access to new markets and information. Thus, traders with a new product, have a cheap and effective way potentially to reach millions of consumers, without needing to invest in physical premises, or contract with middlemen. However this presents the downside that this ease enables dishonest scammers to set up sites, take money, and vanish. It is also harder for enforcers to investigate these online shops, since they may be outside the jurisdiction, and facilitated by intermediaries who will not co-operate. Equally dangerous is where technology may be used by powerful incumbents to stop new entrants from competing.

On the demand side, the internet also allows consumers to access a far wider range of products than they would be able to find on the high street. However where their search results are skewed (for example by search engine optimisation tools used in bad faith), they may end up in the wrong place, and the wrong trader gets their business.

The internet enables unprecedented amounts of information to be used to shape decision making –both by consumers and businesses. So while consumers can research products that might suit their needs, traders can use technology to research their consumers! The use of cookies, IP recognition and so on allows traders to gather instant feedback on their customers, and to access huge stores of big data that can enable them to improve their offering. This brings efficiencies, but can be perceived as creepy by consumers and an invasion of their privacy – and so seriously damage trust, so that markets involving the information economy fail to grow. In this way, false information that leads consumers astray is perhaps only marginally worse than comprehensive and secret information collection about consumers by traders.

4. Driving Competition and Trust

In order to rectify these problems, there are a number of structural and market behaviours that businesses need to get right.

i) Platforms and intermediaries need to take responsibility for the conduct of third party traders using their facilities. Ideally they would offer guarantees when things go wrong.

It is harmful and detrimental to the whole economy when Internet Service Providers refuse to disclose the identity of the persons behind trading websites –especially given that this information is meant to be in the public domain anyway. Where platforms benefit financially from the sales that take place on their websites, they need to ensure that the traders supplying the products act lawfully.

ii) Consumers should not face surprise bills. This means that payments should only be taken when the account holder has given actual, properly informed permission. Payments should not be taken repeatedly when it is clear that the consumer did not mean to consent to this.

iii) While firms have a legitimate interest in managing their reputation, it is important that they adopt a laissez faire approach to positive and negative reviews online published by others. They should not attempt to remove negative reviews, and should not pay for positive reviews.

iv) Transparency about the deal is vital: adverts and terms should be clear, but in addition, if part of the deal is that the user's personal or other data is collected for monetising, this should be made very clear, so that the consumer can actually agree to this transaction. Without this, trust in the potentially lucrative market for personal data is likely to evaporate, leading to consumers exiting the market.

v) Traders should similarly not abuse high tech. Apps and websites should not use cookies, geolocation or personalisation in a way that is intransparent or misleading. While firms may derive a short term gain from this, in the long term the damage to consumer trust is likely to prevent the market from expanding as much as it should, and products that offer a useful service based on geolocation, or personalisation for instance, may find it hard to become established.

vi) Once the deal is made, traders should not try to change it. It is a problem when a contract is unilaterally varied – even when there is an obscure term that purports to permit this – again because this damages trust. It is neither realistic nor efficient to expect consumers to read all the small print: business would grind to a halt if they did. Therefore the terms should conform to the expectations of the contract created by the advertising and headline claims – traders should not seek to hide surprising or onerous features in the small print.

vii) Where something goes wrong, it should be dealt with effectively – a firm that aims to cut costs by providing an incompetent customer service system also damages trust generally, since this is an area that it is hard for consumers to assess up front.

All of the above practices need to be underpinned by effective enforcement. So how well are EU enforcers geared up to achieve this?

5. Barriers to Effective Enforcement

There are four broad areas where enforcers face particular challenges: capability,

international collaboration, jurisdiction, legal issues.

The Capability challenge is partly due to the volume of enforcement work that ideally needs to be done, as set against the level of resource actually available. This can be alleviated by the existence of effective self regulation, but ultimately requires robust prioritisation, so that public resources are directed where they can derive most benefit (meaning that every euro spent on enforcement delivers a substantial return in economic growth). However this is not the full story. Online enforcement involves specialist skills and knowledge not just of the technology, but also of the market and key operators in the industry. There is a need for a step change in enforcement techniques, and significant investment in IT skills and equipment. Enforcers need to carry out detailed analysis of developments (such as the OFT's 2010 work on *Online Targeted Advertising*, and its 2012 call for information on *Personalised Pricing*), but they also need to pool their efforts and knowledge – as the CPC network has been doing through the *Common Activity* projects aimed at building internet enforcement capability in the EU, and the *E-Enforcement Expert Group* launched in April 2014.

We cannot limit our horizons to the EU. Much online activity either originates elsewhere, or has some connection with businesses outside the EU – for example a website directed at consumers in Germany may be registered with a Registry in the USA, via a Registrar in India, hosted on servers in Hong Kong, and supplying goods that are shipped from China. The ultimate trader behind the website may be from anywhere in the world. Taking effective action against such a person (from identifying who they are, to stopping any misspelling they are carrying out) is likely to require investigative assistance from overseas partners, as well as a high level of internet investigation skill. In our global economy, it is also very common for EU consumers to deal with multinational companies, whose policies may be heavily informed by US law, and who may apply specifically EU law inconsistently or not at all in the EU. In order to deal with this effectively, it is imperative that EU enforcers agree common positions and have a shared sense of priorities (working with ECCs and national consumer associations to achieve these), but also that we develop strong relationships of trust with our overseas partners (such as the US Federal Trade Commission), within which we can share complaints and case information, and try to find consistency on the harm, legal arguments and evidence gathering. In short our enforcement cases need to be run as "International projects". Finally, and importantly, we need to be willing to do our bit to protect overseas consumers when harmed by EU based traders too.

"International Jurisdiction" is an important feature of investigations and take downs, but this is pertinent also within the EU. A crucial component in an internet investigation is identifying who is behind a specific website, phone number, social media account or payment account (etc.). Access to this information is rightly restricted, in order to protect the privacy of ordinary people, but it should not be restricted where one is dealing with a trading website – the identity and address of whose operator should be in the

public domain pursuant to the E-Commerce Directive anyway. Likewise, while freedom of speech considerations rightly protect websites from oppressive removal, the same concerns ought not to apply where a website or other account is being used to defraud unsuspecting consumers. An investigation into the full extent of what a website is doing may require the enforcer to engage in covert interaction with the trader (for example to enter personal data to receive an email, or to carry out a test purchase to see whether the goods arrive) – but what is the correct investigative legal framework that surrounds this?

So the question is whether the law is effective given the technology in fact used to trade in an online, mobile and social media focussed world? And how does consumer law fit with important considerations around human rights, privacy and protections for certain intermediaries. These sorts of fundamental doubts are unhelpful for legal certainty.

There are a number of interesting areas where the law may need to be tested in the near future to resolve doubts that are raised by traders and others about its application.

i) A core concept of the Unfair Commercial Practices Directive (UCPD) is the "transactional decision". Does this include a "click through"?

ii) Where a website is operated by an intermediary, who solicits third parties to sell items directly, are they a trader for the purposes of UCPD, or could they benefit from any of the defences in the E-Commerce Directive?

iii) When the consumer receives a product in exchange for personal data they have supplied, or they are encouraged to supply a product themselves, are they still protected by consumer law?

iv) When terms are hidden away, or simply far too long to read, what is the status of clicking a "read and understood" button?

v) What is the extent of enforcers powers to protect non EU consumers, or to secure redress for consumers who have lost money?

These issues are important. A number of harmful practices which persist online have proven difficult to eradicate, such as subscription traps which rely on concealed terms that contradict headline "free trial" claims; drip pricing, which relies on hooking consumers in with headline pricing that is unattainable; fake reviews, which are hard to identify because it is difficult to find out who is actually behind any specific posting; websites remain difficult to remove even when they are clearly illegal – the cost of acquiring a court order to remove a site being disproportionate to the cost to register a new one.

In conclusion, there is some work for the EU legislator to make online markets work well for consumers, businesses and the EU economy. These areas are to: i) clarify the scope of platform responsibility in the consumer context; ii) extend consumer protection to individuals who supply products to traders; iii) ensure enforcers had clear, robust evidence gathering powers, which are effective given the realities of online trade; iv) provide a straightforward and cheap website take down power where sites are causing direct economic

harm to consumers; v) ensure enforcers have the powers both to protect non EU consumers affected by EU traders, and to secure redress where consumer victims have lost out financially.